534,857

Rec'd PCT/PTO 13 MAY 2005

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) **Organisation Mondiale de la Propriété Intellectuelle**
Bureau international

10/534857

(43) **Date de la publication internationale**
3 juin 2004 (03.06.2004)

PCT

(10) **Numéro de publication internationale**
WO 2004/047362 A1

(51) **Classification internationale des brevets**[7] **: H04L 9/32**

(21) **Numéro de la demande internationale :** PCT/FR2003/003380

(22) **Date de dépôt international :** 14 novembre 2003 (14.11.2003)

(25) **Langue de dépôt :** français

(26) **Langue de publication :** français

(30) **Données relatives à la priorité :**
02/14230 14 novembre 2002 (14.11.2002) FR

(71) **Déposant** *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) **Inventeurs; et**
(75) **Inventeurs/Déposants** *(pour US seulement)* : **CANARD, Sébastien** [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). **GUILLOTEAU, Stéphane** [FR/FR]; 42, avenue du 6 Juin, F-14000 Caen (FR). **MALVILLE, Eric** [FR/FR]; 4, rue Maréchal Foch, F-14400 Bayeux (FR). **TRAORE, Jacques** [FR/FR]; 23, avenue de la Suisse Normande, F-61100 Saint Georges des Groseillers (FR).

(74) **Mandataires : MARTIN, Jean-Jacques.** etc.; Cabinet Regimbeau, 20 rue de Chazelles, F-75847 Paris Cedex 17 (FR).

(81) **État désigné** *(national)* **:** US.

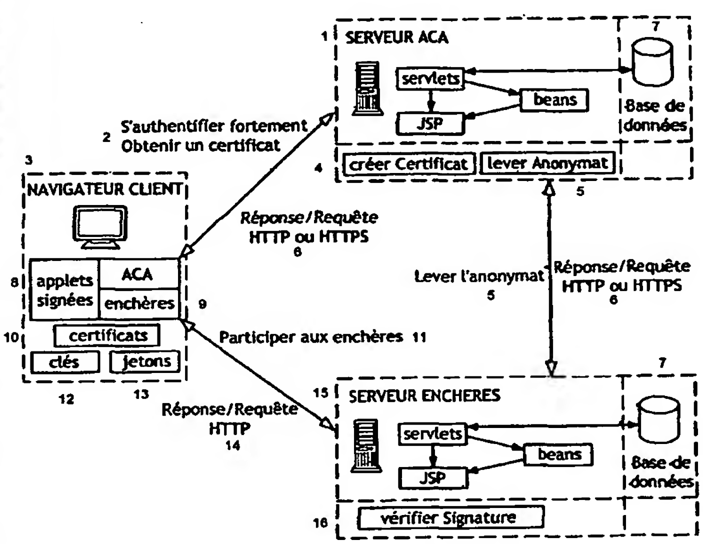
(84) **États désignés** *(régional)* **:** brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

[Suite sur la page suivante]

(54) **Title:** METHOD AND SYSTEM WITH AUTHENTICATION, REVOCABLE ANONYMITY AND NON-REPUDIATION

(54) **Titre :** PROCEDE ET SYSTEME AVEC AUTHENTIFICATION, ANONYMAT REVOCABLE ET NON REPUDIATION



1 ACA SERVER
2 AUTHENTICATE ONESELF STRONGLY OBTAIN A CERTIFICATE
3 CLIENT BROWSER
4 CREATE CERTIFICATE
5 REMOVE ANONYMITY
6 RESPONSE/REQUEST HTTP OR HTTPS
7 DATABASE
8 SIGNED APPLETS
9 AUCTION
10 CERTIFICATES
11 PARTICIPATE IN AUCTION
12 KEYS
13 TOKENS
14 RESPONSE/REQUEST HTTP
15 AUCTION SERVER
16 VERIFY SIGNATURE

(57) **Abstract:** The invention relates to a method of accessing a service. The inventive method consists in: (i) identifying and registering a Client (C), (ii) authenticating the Client with an Anonymous Certification Authority, (iii) authenticating the Client through the production of an anonymous signature and opening and maintaining an anonymous authentication session with a Server (Se) and (iv) selectively enabling a contact between the Server (Se) and the Anonymous Certification Authority (ACA) in order to remove the anonymity of the Client (C) on the basis of the signature supplied in step (iii). The invention also relates to a system of opening and maintaining an authentication session which guarantees non-repudiation.

(57) **Abrégé :** La présente invention concerne un procédé d'accès à un service consistant à $_{ij}$ identifier et enregistrer un Client (C), ii authentifier le Client auprès d'une Autorité de Certification Anonyme, iii) authentifier le Client par la production d'une signature anonyme et ouvrir et maintenir une session d'authentification anonyme auprès d'un Serveur (Se), etiv permettre sélectivement un contact entre le Serveur (Se) et l'Autorité de Certification Anonyme (ACA) pour lever l'anonymat du Client (C) sur la base de la signature fournie à l'étape iii). L'invention concerne également un système apte à permettre l'ouverture et le maintien d'une session d'authentification garantissant la non répudiation.

WO 2004/047362 A1

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE ET SYSTEME AVEC AUTHENTIFICATION, ANONYMAT REVOCABLE ET NON REPUDIATION

DOMAINE TECHNIQUE

L'invention concerne le domaine de la sécurité des accès à des services, notamment à des ressources informatiques.

L'invention a pour objectif général d'offrir un service d'authentification forte et anonyme d'utilisateurs et un mécanisme rapide et économique de maintien de session d'authentification. L'invention permet, malgré l'anonymat, de responsabiliser les utilisateurs en offrant aux ressources la possibilité de lever l'anonymat de l'utilisateur le cas échéant (en cas de litige par exemple).

APPLICATIONS

L'invention peut trouver de nombreuses applications. Celles qui seront indiquées par la suite ne doivent pas être considérées comme limitatives.

Les applications majeures de cette invention sont les enchères électroniques ou les jeux en réseau/communauté. En fait, l'invention est adaptée en particulier à toute application dont le but est de proposer une place publique où plusieurs utilisateurs peuvent se réunir et échanger tout en gardant leur anonymat.

L'invention est particulièrement pertinente pour les enchères électroniques dont le but est de reproduire le principe de fonctionnement des enchères réelles. Les enchères réelles permettent à des personnes, réunies dans une même salle, de faire des offres de manière anonyme. Bien que leur identité réelle ne soit jamais dévoilée, les participants ne peuvent pas se rétracter. La présente invention offre les mêmes propriétés d'authentification anonyme et de non-répudiation.

– Ces mêmes fonctionnalités peuvent également être exploitées pour des applications de jeux multi-acteurs, tels que les jeux de casino, où plusieurs personnes se réunissent autour d'une même table de jeux sans se connaître les uns les autres. Lorsqu'un joueur mise sur un numéro, il ne peut pas nier avoir misé sur ce numéro. La présente invention offre ces propriétés : elle garantit l'anonymat des joueurs

(l'identité des joueurs n'est pas révélée) tout en les responsabilisant (l'identité des joueurs pourra être révélée si besoin).

ETAT ACTUEL DES CONNAISSANCES PUBLIEES SUR LE SUJET (ART ANTERIEUR LE PLUS PROCHE) - INCONVENIENTS DE LA TECHNIQUE ANTERIEURE

Le but général de l'invention est de proposer des moyens permettant 1) de garantir l'anonymat des clients, 2) de maintenir efficacement une session d'authentification et 3) de responsabiliser les clients.

Aujourd'hui, un certain nombre de techniques permettent de répondre en partie à ces exigences, mais aucune n'offre de solution complète à la problématique globale.

Certaines techniques permettent à un serveur d'authentifier un client. Ces techniques sont généralement couplées à un mécanisme permettant de maintenir une session d'authentification entre l'utilisateur et le serveur.

Les techniques majeures offrant des services d'authentification et de maintien de session sont les suivantes : 1) les mots de passe jetables, 2) les techniques SSL et TLS et 3) la technique Kerberos.

- Les mots de passe jetables : le principe des mots de passe à usage unique - encore appelés mots de passe jetables ou OTP (One-Time Password) - consiste à utiliser des mots de passe qui ne peuvent être utilisés qu'une seule fois. Même si le mot de passe est dérobé, il n'est pas réutilisable. Dans la pratique, ce dispositif prend généralement la forme d'une cartulette (ex. ActivCard, SecurID) qui calcule les mots de passe que l'utilisateur doit saisir pour s'authentifier. Ce mot de passe est ensuite utilisé pour calculer une clé de session (une clé secrète) destinée à garantir la confidentialité et l'intégrité des échanges.

- SSL et TLS : ce sont des techniques qui reposent sur des certificats et des algorithmes de cryptographie à clés publiques (ou asymétriques) pour l'authentification et des algorithmes de cryptographie à clés secrètes (ou symétriques) pour le maintien de session. Un certificat constitue une carte d'identité numérique. Il prend

la forme d'un fichier contenant une clé publique et des informations sur son propriétaire. Ces informations sont certifiées (i.e. signées) par une autorité de confiance appelée autorité de certification. Typiquement, pour authentifier un utilisateur, un serveur lui envoie un challenge (une valeur numérique aléatoire) que l'utilisateur signe avec sa clé privée. La clé publique permet au serveur de vérifier que l'utilisateur possède bien la clé privée, le certificat de connaître l'identité de l'utilisateur. En outre, cette phase d'authentification permet au client et au serveur de s'échanger une clé de session (une clé secrète) qui leur permettra de garantir la confidentialité et l'intégrité de leurs échanges.

- Kerberos : il s'agit d'un mécanisme de SSO (Single Sign-On) permettant à un utilisateur d'accéder à plusieurs ressources sans avoir à s'authentifier plusieurs fois. Il repose sur des algorithmes de cryptographie à clé secrète. Typiquement, pour accéder à un serveur, l'utilisateur s'authentifie auprès d'un distributeur de clés ou KDC (Key Distribution Center) qui lui retourne un jeton d'authentification pour ce serveur cible. Ce jeton est envoyé de manière transparente au serveur cible et lui permet d'identifier/authentifier l'utilisateur et de récupérer une clé de session (une clé secrète) utilisée par le serveur et le client pour garantir la confidentialité et l'intégrité de leurs échanges.

Les inconvénients majeurs de ces techniques connues sont les suivants :

- L'anonymat des utilisateurs n'est pas préservé : Les mécanismes d'authentification proposés par ces techniques sont destinés à vérifier l'identité réelle du client. Cette identité est dévoilée par le login dans le cas des mots de passe jetables, par le certificat dans le cas de TLS et SSL ou par le jeton d'authentification dans le cas de Kerberos.

- La non-répudiation n'est pas garantie : Ces techniques s'appuient sur des algorithmes de cryptographie à clé secrète pour maintenir la session d'authentification et garantir la confidentialité et l'intégrité des échanges. Ce type d'algorithme cryptographique ne

permet pas de garantir la non-répudiation ; Le client peut toujours nier avoir envoyé un message.

- Le maintien de la session est coûteux : le maintien de la session est réalisé en chiffrant ou en authentifiant les messages que le client et le serveur s'échangent. Le client doit, en permanence, disposer de moyens de calculs pour maintenir la session.

D'autres techniques offrent des mécanismes d'authentification permettant de préserver l'anonymat des utilisateurs.

L'utilisation d'un pseudonyme est l'approche la plus couramment utilisée par les serveurs actuellement déployés sur Internet (ex. les sites d'enchères électroniques, les sites de jeux). Cette technique repose sur un mécanisme d'authentification basé sur l'utilisation d'un login (i.e. le pseudonyme) et d'un mot de passe. Les utilisateurs s'enregistrent généralement auprès du serveur en renseignant un certain nombre d'informations personnelles et en choisissant un pseudonyme et un mot de passe qu'ils devront ensuite présenter pour s'authentifier. Cette approche pose un certain nombre de problèmes :

- Problème d'ergonomie : chaque utilisateur doit s'enregistrer auprès de chacun des serveurs en entrant plusieurs fois les mêmes informations.
- Problème d'anonymat : Les informations personnelles des utilisateurs sont stockées sur chaque serveur. L'anonymat d'un utilisateur est garanti vis-à-vis des autres utilisateurs mais pas vis-à-vis du serveur. L'utilisateur doit donc faire totalement confiance à chacun des fournisseurs de services.
- Problème d'identification et de responsabilisation : les informations renseignées par l'utilisateur ne sont pas ou peu vérifiées. L'utilisateur est authentifié mais faiblement. Il peut donc entrer des informations erronées, se faire passer pour quelqu'un d'autre ou s'enregistrer plusieurs fois en utilisant différents pseudonymes. D'une manière générale, cette approche ne permet pas de responsabiliser l'utilisateur puisque le serveur ne peut rien prouver.

- Problème de traçabilité : le serveur peut suivre les activités de ses clients et peut ainsi en déduire un profil, information souvent plus intéressante que l'identité réelle. L'anonymat n'est donc pas complètement garanti.

Les techniques de signature de groupe voir documents ([1], [2], [3] et [4] et utilisées notamment pour les enchères électroniques dans l'article [5]) offrent également un mécanisme d'authentification anonyme. Le principe général consiste, pour un client, à s'inscrire auprès d'une autorité de confiance, le gestionnaire du groupe. Les clients enregistrés auprès de cette autorité appartiennent à un même groupe et disposent des moyens nécessaires pour signer au nom du groupe. Tout serveur dispose des moyens pour vérifier une signature. La vérification d'une signature consiste, en fait, à vérifier qu'elle a bien été produite par un membre du groupe ; Elle ne dévoile rien sur le membre qui l'a produite et ne permet donc pas au serveur de connaître son identité. L'anonymat des clients est donc garanti. Un serveur peut, néanmoins, interroger le gestionnaire de groupe pour lever l'anonymat du signataire.

Cette technique répond donc à la problématique d'authentification anonyme. En revanche, elle n'intègre aucun mécanisme permettant de maintenir une session d'authentification entre un client et un serveur. Le serveur ne peut donc pas se "souvenir" de l'identité du client. Pour maintenir l'authentification, le client doit signer chacun des messages qu'il transmet au serveur et doit donc disposer en permanence des moyens de calcul nécessaires. De plus, les calculs mis en œuvre pour réaliser de telles signatures sont assez conséquent et ne permettent pas une authentification rapide.

BUT DE L'INVENTION

Un but de l'invention est de fournir une solution complète à la problématique d'authentification anonyme et de maintien de session.

BASE DE L'INVENTION

Le but précité est atteint dans le cadre de la présente invention grâce à un procédé qui comprend les étapes consistant à :

i) identifier et enregistrer un Client et lui fournir des moyens lui permettant de s'authentifier auprès d'une Autorité de Certification Anonyme,

ii) authentifier le Client auprès de l' Autorité de Certification Anonyme sur la base des moyens fournis en i) et fournir des moyens lui permettant de s'authentifier de manière anonyme auprès d'un Serveur ,

iii) authentifier le Client par la production d'une signature anonyme et ouvrir et maintenir une session d'authentification anonyme auprès d'un Serveur, et

iv) permettre sélectivement un contact entre le Serveur et l'Autorité de Certification Anonyme pour lever l'anonymat du Client sur la base de la signature fournie à l'étape iii).

L'étape i) consiste avantageusement pour un Client utilisateur à récupérer, auprès de l'Autorité de Certification Anonyme formant un tiers de confiance, les informations (une clé publique et un certificat) lui permettant de calculer des signatures anonymes. Tout serveur ou ressource peut vérifier ces signatures sans que l'identité réelle de l'utilisateur ne lui soit révélée. Une signature valide garantie à la ressource ou serveur qu'il pourra, le cas échéant, recouvrer l'identité réelle de l'utilisateur en interrogeant le tiers de confiance.

La présente invention propose ainsi une solution complète et globale pour :

- Garantir l'anonymat des clients : l'invention repose sur des mécanismes d'authentification forte permettant de préserver l'anonymat des clients ;
- Maintenir efficacement une session d'authentification : le mécanisme de maintien de session d'authentification que propose l'invention ne nécessite aucun calcul côté client. Toutes les informations nécessaires sont calculées au cours de la phase d'authentification ;
- Responsabiliser les clients : L'invention permet de garantir la non-répudiation. D'une part, parce qu'à tout moment, le serveur peut lever l'anonymat d'un client en interrogeant un tiers de confiance.

D'autre part, parce que le serveur peut prouver chacune des actions d'un client.

La présente invention concerne également un système apte à permettre l'ouverture et le maintien d'une session d'authentification garantissant la non répudiation, caractérisé par le fait qu'il comprend des moyens adaptés pour la mise en œuvre de trois phases :

. une première phase dans laquelle un Client calcule un ensemble de données, formé d'une suite de jetons, l'un de ceux-ci permettant d'ouvrir une session, tandis que les autres permettent de la maintenir,

. une deuxième phase dans laquelle le Client s'engage fortement sur la suite de jetons après d'un Serveur, et

. une troisième phase de maintien de la session à l'aide de la suite de jetons.

On notera que dans le contexte de ce système d'ouverture et de maintien de session, le Client dispose de moyens lui permettant de produire une signature digitale qui n'est pas obligatoirement anonyme, bien que préférentiellement elle le soit bien entendu.

Les documents [12], [13] et [14] décrivent diverses modalités d'enchères électroniques. Aucun de ces documents n'enseigne ni ne suggère une ouverture et un maintien de session, permettant des interventions multiples successives du client, au sein de la même session résultant d'une seule et unique authentification initiale. En effet, selon les modalités définies dans chacun de ces documents, les enchérisseurs n'envoient qu'une seule valeur ou donnée.

D'autres caractéristiques, buts et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui va suivre, et en regard des dessins annexés, donnés à titre d'exemples non limitatifs et sur lesquels :

- la figure 1 représente l'architecture générale des moyens relationnels mise en jeu dans le cadre de la présente invention,

- la figure 2 représente un organigramme schématique du procédé conforme à la présente invention,

- la figure 3 schématise le processus d'identification forte,

- la figure 4 schématise le processus de certificat anonyme,
- la figure 5 schématise le processus de signature aveugle à anonymat révocable,
- la figure 6 schématise le processus de signature de groupe,
- la figure 7 schématise l'application de la présente invention à un processus d'enchères électroniques,
- la figure 8 schématise une étape préparatoire de mise en vente et consultation dans le contexte d'enchères électroniques,
- la figure 9 schématise un exemple de fiche article mise à disposition d'un visiteur, Client potentiel, dans le cadre d'une vente aux enchères,
- la figure 10 schématise une étape d'obtention de certificat anonyme,
- la figure 11 schématise les étapes d'inscription de groupe, génération de clés et envoi de certificat dans ce contexte,
- la figure 12 schématise une étape de demande de participation avec certificat et autorisation,
- la figure 13 schématise les étapes d'initialisation puis de génération de jetons par deux Clients respectifs dans le cadre d'enchères,
- la figure 14 schématise une étape de participation à une vente aux enchères,
- la figure 15 schématise les étapes de surenchères par transmission de jeton dont l'indice (ou "rang") représente la valeur choisie pour la surenchère,
- la figure 16 schématise une étape de traitement des ordres d'enchères,
- la figure 17 schématise le traitement d'un jeton reçu d'un Client et la comparaison de la valeur représentée par son indice avec les données antérieurement reçues,
- la figure 18 schématise une étape de conclusion de vente aux enchères,
- la figure 19 schématise des étapes d'information de Client gagnant d'enchères, de Clients perdant, de vendeur et de fin de transaction, et
- la figure 20 schématise une architecture Client-Serveur permettant de mettre en oeuvre le procédé à la présente invention.

Comme indiqué précédemment et illustré sur la figure 1 annexé, l'invention met en oeuvre trois entités dans le protocole : des Clients C, au moins une Autorité de Certification Anonyme ACA et au moins un Serveur (ou "Ressource") Se.

Comme également indiqué précédemment, l'invention propose, d'une part, un mécanisme d'authentification anonyme basé sur l'utilisation de certificat anonyme. Elle propose, d'autre part, un mécanisme de maintien de session économique et efficace garantissant la non-répudiation. Enfin, elle propose une solution globale combinant les mécanismes d'authentification anonyme (ex. signature de groupe, certificat anonyme) et le mécanisme de maintien de session pour répondre aux problématiques suivantes :

- L'anonymat des utilisateurs : l'invention repose sur des mécanismes d'authentification forte permettant de préserver l'anonymat des utilisateurs, non seulement vis-à-vis des autres utilisateurs, mais aussi vis-à-vis des serveurs ;
- L'efficacité et portabilité : le mécanisme de maintien de session d'authentification que propose l'invention ne nécessite aucun calcul côté utilisateur. Toutes les informations nécessaires sont calculées préalablement au cours de la phase d'authentification ;
- La non-répudiation : L'invention permet de garantir la non-répudiation. D'une part parce qu'à tout moment, le serveur peut lever l'anonymat d'un utilisateur en interrogeant le tiers de confiance ACA. D'autre part parce que le serveur peut prouver chacune des actions d'un utilisateur.
- L'ergonomie : l'utilisateur s'enregistre une seule et unique fois auprès d'un tiers de confiance ACA.

L'Autorité de Certification Anonyme (ACA) délivre des certificats anonymes et est adaptée et habilitée pour lever l'anonymat le cas échéant. Le Serveur fournit des services à des personnes C désirant rester anonyme, cet anonymat pouvant être levé quand cela est nécessaire. Un Client va obtenir un certificat anonyme dans le but de

s'authentifier anonymement puis de maintenir une session auprès d'un Serveur.

Le procédé conforme à l'invention dans une mise en oeuvre préférentielle comprend essentiellement 4 étapes.

• Etape 1 : l'identification. Le Client C s'enregistre auprès d'une autorité de confiance (cette autorité peut être soit l'Autorité de Certification Anonyme elle-même, soit une autorité de certification). Cette étape consiste pour l'utilisateur à fournir des informations personnelles (nom, prénom, adresse, etc .). Plusieurs alternatives sont possibles pour cela. Par exemple, le client peut s'enregistrer soit en ligne en remplissant un formulaire électronique, soit en se déplaçant physiquement dans un endroit bien précis. L'autorité de confiance vérifie l'identité du client et toutes ou une partie de ses informations personnelles, stockent ces informations pour une utilisation future et fournit au Client les moyens (par exemple un login/mot de passe ou un certificat) qui lui permettront de s'authentifier auprès de l'ACA. Il est à noter que dans tout le reste du protocole, le Client ne fournira plus à aucun moment ses données personnelles.

• Etape 2 : l'authentification auprès de l'ACA. Cette étape met en jeu le Client et l'ACA. Le Client s'authentifie de manière forte auprès de l'ACA (en utilisant les moyens qu'il a obtenus à l'étape 1). L'ACA lui délivre en retour les moyens de produire une signature anonyme. Elle se garde les moyens de pouvoir relier à tout moment le Client (i.e. la personne physique qu'elle connaît à l'aide de l'authentification forte) à n'importe quelle signature émanant de celui-ci.

• Etape 3 : l'authentification anonyme auprès du Serveur. Cette étape met en jeu un Serveur et un Client. Ce dernier désire maintenir une session pour accéder aux services qu'offre le Serveur et doit pour cela faire savoir à ce dernier qu'il s'est authentifié de manière forte auprès de l'ACA. Pour autant, le Client veut rester anonyme vis-à-vis du Serveur et d'autres clients potentiels. Le but de cette étape est d'ouvrir une session auprès due Serveur en faisant un certain nombre de calculs pour ensuite pouvoir maintenir cette session de manière très rapide.

Cette étape va ainsi se diviser en trois phases. La première phase va permettre au Client de calculer un ensemble de données (une suite de jetons), l'un de ces jetons permettant d'ouvrir la session alors que les autres permettront de la maintenir. La deuxième phase permettra au Client de s'engager fortement sur cette suite de jetons auprès du Serveur. La troisième phase consistera à maintenir la session à l'aide de cette suite.

Remarque 1 : Dans certains cas (par exemple lorsque le service d'anonymat est facturé aux serveurs), l'ACA peut exiger une authentification des Serveurs qui veulent offrir le service d'anonymat à leurs utilisateurs. Pour cela, l'ACA doit pouvoir exiger une authentification des serveurs avant de remettre un certificat anonyme à l'utilisateur et/ou avant de lever l'anonymat. Les serveurs doivent donc préalablement se soumettre à une phase d'enregistrement auprès de l'ACA. Pour cela, chaque serveur fait une demande d'affiliation à l'ACA qui étudie la proposition (suivant des critères qu'elle a établis) et décide d'accepter ou non la proposition.

Remarque 2 : Les deux premières phases nécessitent un dialogue entre l'utilisateur et l'ACA d'une part (première phase), et entre l'utilisateur et le serveur d'autre part (seconde phase). Elles seront donc typiquement réalisées en utilisant un navigateur web ou une application hébergée sur le poste du client. Toutefois, puisque la suite de jetons est pré-calculée au cours de la phase d'authentification, elle peut être embarquée dans un terminal portable (téléphone mobile, PDA, ...). L'utilisateur peut donc s'authentifier auprès du serveur en utilisant un navigateur ou une application et maintenir ensuite la session d'authentification en utilisant un autre type de terminal.

Tous les jetons sont à usage unique et sont fortement dépendants les uns des autres. Ils ne peuvent être calculés que par le Client et sont non-falsifiables. N'importe qui, et en l'occurrence le Serveur, peut vérifier la dépendance (et donc la provenance) de ces jetons.

Dans un premier temps donc, le Client, au cours de l'ouverture de la session, calcule la suite de jetons. L'algorithme de génération des jetons est basé sur l'utilisation de deux primitives cryptographiques : une fonction de hachage et un nombre aléatoire.

Une fonction de hachage H() possède les propriétés suivantes :

– H(M) opère sur un message M de longueur arbitraire

– Le résultat h = H(M) possède une longueur l fixe

– Etant donné M, il est facile de calculer h

– Etant donné M, il est difficile de trouver un autre message M_0 tel que $H(M) = H(M_0)$

Parmi les fonctions de hachage, nous pouvons citer MD5 ("Message Digest 5") ou SHA ("Secure Hash Algorithm"). SHA produit une sortie de 160 bits appelée message abrégé.

Afin d'initialiser l'ensemble des jetons, il est nécessaire de générer un nombre aléatoire à partir duquel la fonction de hachage va calculer les jetons. Ce nombre aléatoire doit être cryptographiquement sûr, c'est-à-dire qu'il faut que la probabilité de réussite de la recherche exhaustive soit quasi nulle.

La fonction de hachage appliquée à ce nombre aléatoire W_0 permet d'obtenir un résultat W_1 (c'est-à-dire un premier jeton) auquel on applique à nouveau la fonction de hachage pour obtenir un deuxième jeton W_2 et ainsi de suite pour obtenir n jetons :

$H(W_0) = W_1, \ldots, H(W_{n-1}) = W_n$

La suite de jetons est donc $(W_n, W_{n-1}, W_{n-2}, \ldots, W_1, W_0)$. Du fait des propriétés des fonctions de hachage, il est facile, à partir de W_0, de calculer n'importe lequel des W_i (pour i allant de 1 à n) alors qu'il est impossible en pratique de retrouver W_0 à partir des W_i (pour i allant de 1 à n).

Dans un second temps, le Client utilise ses moyens d'authentification forte anonyme obtenus à l'étape 2 pour produire une signature anonyme du jeton d'initialisation Wn, la signature permettant au serveur d'authentifier ce Client (il peut vérifier la validité de la signature et donc être convaincu des droits du client qu'il a en face de

lui). Le Client vient ainsi d'ouvrir une session anonyme auprès du Serveur. Il va pouvoir maintenir cette session à l'aide de la suite de jetons. Le jeton W_n est stocké par le Serveur et sera utilisé pour vérifier la validité des autres jetons (et donc de la session).

Remarque : Au cours de la phase d'authentification anonyme, un certain nombre d'informations peuvent être associées au jeton d'initialisation (par exemple, la valeur numéraire d'un jeton). Ces informations constituent les informations de session et permettent de décrire la sémantique associée à chaque jeton. Un jeton permettra donc au serveur de retrouver l'identité de l'émetteur mais également les informations de session.

Au cours de la session, le Serveur veut être sûr de pouvoir retrouver l'identité physique du client qu'il a en face de lui, selon le principe défini à la quatrième étape. De plus, il faut que cette authentification se fasse rapidement. Pour cela, le Client transmet simplement, à chaque nouvelle authentification, un jeton de la liste calculée précédemment : W_{n-1}, puis W_{n-2},W_{n-3}, ... Pour poursuivre la session, le Client transmet ainsi les jetons dans l'ordre de n − 1 à 0.

D'une manière générale, si le résultat de $h(W_{n-1})$ est bien égal à W_n alors l'authentification est acceptée. Le Serveur est capable de vérifier ce lien : le jeton W_l reçu est comparé avec les jetons de l'ensemble des clients présents dans la base. Ainsi, pour trouver dans la base le W_k relié au W_l reçu, il utilise la formule : $h^1(W_l) = W_k$ (en utilisant le fait que $h^2(W_{n-2})=h(h(W_{n-2}))=h(W_{n-1})=W_n$). Si le Serveur parvient à trouver dans sa base ce jeton W_k, alors il accepte la poursuite de la session et le jeton W_l remplace le jeton W_k pour la vérification suivante. Dans le cas contraire, le jeton n'appartient pas à un client et l'authentification est refusée.

Lors des diverses authentifications se déroulant au cours de la session, le Serveur sait ainsi toujours relier un jeton (et donc la session) à la signature anonyme effectuée au moment de l'ouverture de cette session.

• Etape 4 : Elle met en jeu un Serveur et l'Autorité de confiance. Le premier a en sa possession une signature qu'il sait émanant d'un Client s'étant identifié de manière forte auprès de l'ACA. S'il le souhaite, il peut donc envoyer cette signature à l'ACA qui a les moyens de découvrir l'identité physique du signataire (cf. première étape) et de fournir cette information au Serveur. Ce dernier peut ainsi obtenir l'identité physique du Client ayant produit la signature et l'ensemble des jetons qu'il a reçu au cours de sa session.

Une variante consiste à faire en sorte que le Serveur ne connaisse à aucun moment l'identité du Client. Dans ce cas, une fois la levée d'anonymat effectuée par l'ACA, ce dernier contacte personnellement le Client impliqué et termine ainsi la session de la manière adéquate.

Dans certains cas, le droit de production de signature anonyme a une durée de vie limitée (par exemple liée à une seule session). Dans ce cas, le Client devra s'authentifier de manière forte auprès de l'ACA à chaque session (i.e. pour chaque suite de jeton).

Le nombre de sessions liées à un engagement est limité dans le temps. En effet, la suite de jetons est finie. Une fois le dernier jeton envoyé, le Client doit produire une nouvelle suite de jetons auprès du Serveur et doit signer anonymement le jeton d'initialisation.

D'autre part, l'étape 3 peut être utilisée seule pour ouvrir et maintenir efficacement une session d'authentification. Ainsi, un Client va pouvoir s'authentifier de manière forte auprès du serveur (mais sans anonymat cette fois-ci) et maintenir une session, de manière très rapide, à l'aide de la suite de jetons qu'il aura préalablement calculés. Cette approche permet, en outre, de garantir la non-répudiation.

DESCRIPTION DETAILLEE D'UN MODE DE REALISATION

Spécification du mécanisme de jetons

Jeton d'initialisation

Le premier jeton envoyé par le Client au Serveur est appelé jeton d'initialisation et permet d'ouvrir la session. Il est lié, à la fois, à l'authentification du Client à partir d'une signature et aux informations

de session. Ainsi, le jeton d'initialisation fixe par association, dans un message envoyé par le Client au Serveur, la preuve d'authentification et les paramètres d'initialisation de la session.

Dans le cas des enchères, dont l'application est décrite par la suite, le mécanisme de jetons est utilisé dans la phase de participation à une vente. Un Client demande une participation à la vente aux enchères en transmettant un message composé du jeton d'initialisation associé aux paramètres de la vente, par exemple, l'identifiant de l'article, son prix actuel, et la valeur du pas. C'est ce message qui est signé. Le Client transmet également, dans cette demande de participation, les moyens pour le serveur de vérifier la signature (message, clé publique, certificat...) et donc d'authentifier le Client, en fonction du mécanisme de signature utilisé. Des spécifications du mécanisme de signature seront décrites ci-dessous.

Si l'authentification du Client par le Serveur est valide, le jeton d'initialisation et les données transmises par le Client, dans cette demande de participation, sont enregistrés par le Serveur d'Enchères.

Jetons de maintien de session

Dans le cas des enchères, si le Serveur autorise le Client à participer à la vente après avoir reçu le jeton d'initialisation, le Client peut alors surenchérir en envoyant au Serveur les jetons successifs et seulement les jetons. En effet, chaque ordre d'enchère du Client se traduit par l'envoi d'un jeton sans autre information ni signature. A partir des informations enregistrées avec le jeton d'initialisation, le Serveur est capable d'authentifier l'ordre en attribuant le jeton à son Client propriétaire et de calculer sa valeur. Ainsi, chaque jeton reçu par le Serveur est comparé avec l'ensemble des jetons enregistrés. Par dépendance entre jetons, ~~le~~ nouveau jeton reçu par le Serveur ne peut correspondre qu'à un seul jeton présent dans la base. Le Serveur retrouve les informations sur le Client et sur l'article lié au jeton reçu en le mettant en correspondance avec un jeton stocké et un seul. Selon ce procédé, le mécanisme de jetons peut s'appliquer aux enchères en établissant des règles de calcul.

Côté client, le calcul de l'indice i du jeton Wi pour surenchérir (prixsup) est basé sur le prix actuel de l'article (prixmax) et du pas de l'article (pas). Les formules peuvent être :

prixsup = prixmax + pas

j = (prixsup - prixdedepart)/pas

i = nombretotaldejetons – j

Côté serveur, le jeton W_l reçu est comparé avec les jetons présents dans la base. Les formules permettant de retrouver le jeton et de calculer sa valeur peuvent être :

– Pour trouver dans la base W_k, la formule est : $h^l(W_l) = W_k$

– Pour calculer la valeur de W_l, la formule est : W_l = prixdeW_k + (l *pas)

Spécification du mécanisme de signature du jeton d'initialisation.

La signature du jeton d'initialisation permet l'ouverture d'une session et peut être réalisée, selon les cas, avec ou sans anonymat. Le Client possède une clé privée SK, une clé publique PK et un certificat (anonyme ou non). Il utilise sa clé privée SK et un algorithme cryptographique (par exemple RSA, DSA ou signature de groupe) pour signer un message composé du jeton d'initialisation Wn et des informations de session session_data. Il obtient ainsi une signature S-Sigsk (Wn, session_data) qu'il envoie au Serveur avec le message, sa clé publique PK et le certificat C qui relie cette clé publique à son identité propre.

La figure 3 schématise les détails du protocole de signature du jeton d'initialisation.

Spécification des mécanismes de signature anonyme.

Certificat anonyme

Lors de la seconde étape, le Client C crée une paire de clés publique PK – privée SK (par exemple des clés RSA). Il garde secret la clé privée et envoie à l'ACA la clé publique PK afin d'obtenir, lors d'une session authentifiée fortement, un certificat AC=Sig_{ACA} (PK, Pseudo) de cette clé liée à un pseudonyme choisi par l'ACA et/ou le Client. Ce pseudonyme peut éventuellement être le chiffrement de la véritable

identité du Client accompagnée d'un aléa. La levée de l'anonymat se fait ainsi facilement par l'ACA qui déchiffre ce pseudonyme pour obtenir l'identité du Client. L'ACA garde en mémoire le lien entre le Client et son pseudonyme pour, par la suite, pouvoir lever l'anonymat.

Remarque : D'une manière générale, un certificat anonyme permet de lier un pseudonyme à une clé publique. Mais il peut également, en fonction du contexte, contenir d'autres informations permettant de limiter la portée du certificat (ex. l'identifiant du serveur, l'identifiant d'une session, une date de validité, l'adresse IP du client, le contexte d'authentification ...).

L'étape de signature du jeton d'initialisation consiste pour le Client à utiliser sa clé privée PK (il s'agit donc d'une signature RSA). Le message est constitué du jeton d'initialisation W1000, de la signature S, de la clé publique PK et du certificat lié au pseudonyme AC+Pseudo. Le Serveur ouvre donc une session avec un client qu'il ne connaît que sous un pseudonyme. Il vérifie ainsi que le Client s'est authentifié fortement auprès de l'ACA à l'aide du certificat AC et que la clé publique PK certifiée (et appartenant au pseudonyme) permet bien de vérifier la signature du jeton d'initialisation.

La levée de l'anonymat est mise en œuvre lorsque le Serveur fournit à l'ACA le certificat (ou le pseudonyme). L'ACA peut savoir à quel Client correspond ce pseudonyme et donc qui a produit la signature.

La figure 4 schématise les détails des protocoles de certificat anonyme.

Il est à noter que pour obtenir un anonymat intéressant, il convient de changer de certificat (et donc de paire de clé de signature) à chaque session. Il faut donc que le Client se connecte à l'ACA à chaque session.

Remarque : si le Client désire se connecter à plusieurs serveurs bénéficiant des services de l'ACA, au moins deux possibilités s'offrent à lui. Soit l'ACA fournit un seul certificat (universel) pour l'ensemble des serveurs, auquel cas il est possible de tracer le pseudonyme de ce Client sur l'ensemble des sites (on ne sait pas qui il est mais on sait ce qu'il

fait sur chacun des serveurs). Soit l'ACA fournit un certificat par serveur , auquel cas on perd l'universalité du certificat mais il est alors impossible de tracer un même client sur plusieurs serveurs.

Chaque serveur fournit au Client un identifiant qui est retransmit à l'ACA. Ce dernier sait alors qu'il a fournit à tel Client un certificat pour tel Serveur et donc n'en fournira pas deux.

Remarque : de même, si le Client possède deux machines à partir desquelles il désire accéder au Serveur (par exemple une machine à son lieu de travail et une machine chez lui), il doit pouvoir obtenir deux certificats différents de la part de l'ACA.

Certificat aveugle à anonymat révocable

Une partie du processus conforme à la présente invention peut s'apparenter à un certificat aveugle à anonymat révocable.

Le concept de schéma de signature aveugle a été introduit par Chaum à Crypto'83. Un schéma de signature aveugle est un protocole mettant en jeu deux entités : un signataire et un utilisateur. Il permet à l'utilisateur d'obtenir la signature d'un message donné faite par le signataire, sans que ce dernier n'apprenne quoi que ce soit à propos du message.

Le modèle de la signature aveugle à anonymat révocable est constitué de plusieurs utilisateurs, d'un signataire, d'une autorité reconnue, par exemple un juge, et de deux protocoles :

- Un protocole de signature entre le signataire et l'utilisateur.
- Un protocole de recouvrement entre le signataire et le juge.

A l'aide du protocole de signature, l'envoyeur obtient une signature valide du message de son choix de telle sorte que le signataire ne peut pas relier le protocole et la paire message/signature. Il existe deux types de signature aveugle à anonymat révocable, suivant l'information que le juge reçoit du signataire pendant le second protocole :

- Révocation de type 1 : à l'aide de la partie du protocole venant du signataire, le juge donne l'information qui permet au signataire (ou à

n'importe qui) de reconnaître le message (i.e. le juge peut retrouver le message).

– Révocation de type 2 : à l'aide du message et de la signature, le juge permet au signataire de retrouver efficacement l'utilisateur ou la partie du protocole correspondant à la signature.

On se reportera aux documents [6], [7], [8], [9], [10] et [11] pour disposer d'exemples de schéma de signature aveugle à anonymat révocable (en anglais "fair blind signature").

Dans le cas de l'invention (révocation de type 2), l'ACA joue le rôle du signataire et le Serveur joue celui de juge. Le Client est l'utilisateur. Lors de la première étape, le Client crée une paire de clés publique PK – privée SK (par exemple de type RSA). Il garde secret la clé privée de signature et envoie à l'ACA la clé publique PK afin d'obtenir, lors d'une session authentifiée fortement, une signature aveugle BC à anonymat révocable (protocole d'obtention de certificat) de cette clé (la signature aveugle correspond à son certificat anonyme). L'ACA garde en mémoire les moyens de lever l'anonymat de cette signature. Sur la figure 5, cette signature aveugle est intitulée $BC=BSig_{ACA}$ (PK).

L'étape de signature du jeton d'initialisation (protocole de signature de jeton) consiste pour le Client à utiliser sa clé privée PK pour signer (il s'agit donc d'une signature RSA). Le message est constitué du jeton d'initialisation W1000, de la signature S, de la clé publique PK et du certificat anonyme BC. Le Serveur vérifie ainsi que le Client s'est authentifié fortement auprès de l'ACA à l'aide du certificat anonyme (il vérifie que la signature BC émane bien de l'ACA) et que la clé publique PK certifiée permet bien de vérifier la signature S du jeton d'initialisation.

La levée de l'anonymat est mise en œuvre lorsque le Serveur fournit à l'ACA le certificat anonyme BC. L'ACA peut savoir à quel moment il a produit cette signature (protocole de levée d'anonymat) et donc à qui est ce qu'il l'a fourni.

La figure 5 schématise les détails des protocoles de certificat aveugle à anonymat révocable.

Il est à noter que dans ce cas, il convient d'obtenir une signature aveugle pour chaque session (il est ainsi impossible de relier deux sessions d'un même client). Il faut alors que le Client se connecte à l'ACA avant chaque début de session.

On retrouve le même problème (et les mêmes solutions) que pour le certificat anonyme dans le cas de plusieurs serveurs ou de plusieurs machines par client.

Certificat de groupe

L'invention peut également mettre en oeuvre une signature de groupe.

Une signature de groupe permet aux membres d'un groupe de produire une signature telle que le vérificateur reconnaîtra cette signature comme ayant été produite par un membre du groupe, tout en ignorant de quel membre il s'agit. Cependant, une autorité de confiance a la possibilité de lever à tout moment cet anonymat et donc de révéler l'identité du signataire. De telles signatures sont bien souvent "non-corrélables" : il est impossible de déterminer si deux signatures ont été émises par la même personne ou non.

Dans tout schéma de signature de groupe, est attribuée au groupe une unique clé publique de groupe, tandis que sont attribués à chaque membre de ce groupe un identifiant et une clé privée qui lui sont propres. A l'aide de sa clé privée, un membre du groupe peut produire une signature de groupe d'un message de son choix, laquelle signature peut être vérifiée par une entité quelconque à l'aide de la clé publique de groupe. La vérification apprend seulement à cette entité que la signature a été produite par un membre du groupe, mais ne lui donne aucune information sur l'identifiant du membre qui a signé. En revanche, l'autorité de confiance dispose d'une information supplémentaire qui lui permet de retrouver l'identifiant de ce membre, et donc de lever cet anonymat à tout moment (on dit que l'autorité de

confiance "ouvre" la signature). On se reportera aux documents [1], [2], [3] et [4] pour des schémas de signature de groupe.

Dans le cas de l'invention, l'ACA joue le rôle d'autorité de confiance. Au cours de la première étape, un Client va s'inscrire à unn groupe auprès de l'ACA en interagissant avec lui afin d'obtenir un certificat de membre GC (protocole d'enregistrement d'un membre). L'ACA se garde les moyens d'ouvrir une signature le cas échéant.

L'étape de signature du jeton d'initialisation W1000 consiste à produire une signature de groupe S de cet élément (protocole de signature de groupe) soit $S=Sig_{GP}$ (W1000). Ainsi, le signataire est anonyme au sein du groupe. Le Serveur a les moyens de vérifier qu'une signature a bien été émise par un membre du groupe (protocole de vérification de signature de groupe) mais sans pour autant savoir de quel membre il s'agit.

Enfin, l'ACA, en temps qu'autorité de confiance, a les moyens d'ouvrir la signature (protocole d'ouverture de signature de groupe) pour lever l'anonymat et divulguer l'identité du signataire.

La figure 6 schématise les détails des protocoles de certificat de groupe.

Il est à noter que, du fait des propriétés d'anonymat et de non-reliabilité des signatures de groupe, il n'est pas nécessaire de s'enregistrer au groupe pour chaque session. Le fait d'être inscrit au groupe permet de faire autant de signature de groupe que le Client le désire sans pour autant que quelqu'un puisse relier deux de ses signatures. Ce certificat unique peut être utilisé chez plusieurs serveurs sans risque de pouvoir tracer le client. De même, un client possédant plusieurs machines n'aura pas besoin d'obtenir plusieurs certificats.

Remarque : Une propriété intéressante des approches basées sur les signatures de groupe et les signatures aveugles est qu'elles permettent de répartir les fonctions de génération de certificats et le pouvoir de levée d'anonymat entre deux ou plusieurs autorités. Selon ce principe, la levée de l'anonymat d'un utilisateur ne sera possible que si

l'ensemble de ces autorités l'autorise. Ce processus est moins naturel dans le cas des certifications anonymes.

EXEMPLE DE REALISATION

On va maintenant décrire plus particulièrement l'application de la présente invention aux enchères électroniques.

L'application présentée ici pour illustrer le procédé conforme à l'invention appartient au domaine du commerce électronique sous la forme des ventes aux enchères sur Internet.

Le principe de ventes retenu est celui des enchères classiques où un article est mis aux enchères croissantes entre plusieurs enchérisseurs et pendant un temps déterminé. Cette réalisation s'appuie sur les technologies Java (applet, servlet, jsp) en architecture client-serveur avec un système de gestion de base de données relationnel.

<u>1 Problème spécifique aux enchères résolu par le procédé</u>

1.1 But

Le procédé offre une solution innovante pour sécuriser les enchères électroniques et permettre de réaliser des transactions en toute confiance.

Actuellement, les enchères en ligne ne présentent pas des niveaux de sécurité suffisants dans le cas d'enchères de grandes valeurs et pour des participants scrupuleux de préserver leur anonymat. L'organisation de ventes aux enchères publiques de plusieurs milliers voire plusieurs millions d'euros réclament de nouveaux mécanismes.

La cryptographie utilisée dans le cadre de l'invention permet de répondre aux objectifs. Les informations transmises sont inintelligibles à des personnes extérieures à la transaction pour des raisons de confidentialité.

Le procédé assure la non-répudiation pour garantir que le client ne peut pas nier avoir fait acte de surenchère.

Le procédé assure l'intégrité des données échangées.

Le procédé permet d'assurer l'identité d'un utilisateur par authentification.

De plus, le procédé est rapide pour la prise en compte en temps réel des ordres d'enchères.

1.2 Innovation et avantages techniques du procédé appliqué aux enchères

Le mécanisme de jetons signés avec anonymat est adapté aux enchères. Avec ce procédé, un acheteur peut être autorisé à participer aux enchères sans risque d'infractions liées à la divulgation de son identité. Personne ne peut se faire passer pour un autre et seuls les membres inscrits et autorisés peuvent participer aux enchères.

Le système actuel connu de login/mot de passe est très répandu mais il ne présente pas toutes les garanties. Un programme informatique peut facilement capturer l'information transmise en clair sur Internet et offrir ainsi la possibilité à un usurpateur de voler un mot de passe. Si un protocole comme SSL permet de se prémunir contre ce type d'attaques, il ne permet pas en revanche de lutter contre les attaques à base de dictionnaires de mots de passe. En effet, ces attaques peuvent permettre de casser facilement des mots de passe trop courts et trop simples.

La caractéristique des jetons utilisés dans le procédé conforme à l'invention est son usage unique. Il ne peut servir que pour un ordre d'enchère et un seul, et ne dévoile aucune information sur son utilisateur. Il permet juste de vérifier que la requête transmise appartient bien à un utilisateur précis. Ici, un ordre d'enchère identifié par un mot de passe jetable est certifié appartenir à un acheteur particulier pour une valeur unique.

Les jetons sont envoyés par le client C au serveur d'enchères Se pour enchérir sur un produit. La présentation au début de l'enchère d'un premier jeton, noté W1000 pour le client 1 et X1000 pour le client 2, sert d'initialisation et de preuve pour la suite de la vente (voir figure 7). A partir de ce mécanisme de jetons, le principe est de signer le premier jeton envoyé pour enregistrer la demande de participation d'un client. Les jetons transmis pour enchérir sont vérifiés à partir de ce premier jeton d'initialisation, conformément au processus précédemment décrit.

Les jetons suivants représentent les surenchères. Par exemple, si un client (client 1) participe à une enchère avec un prix de départ à 1000 et un pas à 100, il peut proposer d'enchérir à 1100 en transmettant un jeton (W999). Pour enchérir à 1400 et battre un autre acheteur monté à 1300, il devra révéler le jeton correspondant au prix de 1400 soit le jeton W996.

Ce processus est schématisé sur la figure 7.

2 Modélisation du système

2.1 Schéma général

L'application de ventes aux enchères fait appel aux trois entités définies précédemment dans le procédé :

- L'Autorité de Certification Anonyme (ACA) est placée sur un serveur d'anonymat (SA);
- Le serveur Se fournisseur de services est ici le serveur d'enchères ;
- Le client C.

Nous trouvons également dans cette application un serveur de certificat (SC) qui fournit un certificat pour l'authentification forte.

Les fonctions principales du système d'enchères électroniques sont :

- La phase préparatoire : qui consiste à mettre en vente, consulter et obtenir un certificat anonyme;
- La phase d'enchères : qui consiste à demander et vérifier une participation à une vente, enchérir et vérifier l'enchérissement dans le but d'acquérir un article;
- La phase conclusion : qui consiste à mettre un terme aux enchères, valider et identifier un gagnant en levant l'anonymat, clore la vente.

Chacune de ces fonctions va être détaillée par la suite.

2.2 Mise en vente et consultation

Cette fonction est schématisée figure 8.

- Phase du déroulement : Préparatoire ;

– Niveau de sécurité : Assurer l'authenticité du serveur d'enchères ;

– Précondition : Connaître le site d'enchères ;

– Objectifs : Faire connaître les articles mis en vente ;

– Acteur principal : Visiteur, Vendeur, Administrateur ;

– Scénario typique : M.Martin est un collectionneur d'art, il décide d'acquérir une oeuvre mise en vente sur le site d'enchères. Il se connecte au site et demande à afficher le catalogue des articles à vendre. Parmi les articles, il s'intéresse plus particulièrement à une photographie intitulée Regards dont le prix de départ est 600 euros et vendu par M.LeVendeur. Il clique alors pour obtenir la fiche article, illustré à titre d'exemple sur la figure 9.

2.3 Obtention d'un certificat anonyme

Cette fonction est schématisée sur la figure 10.

– Phase du déroulement : Préparatoire; elle correspond à la première étape du procédé;

– Niveau de sécurité : Obtenir l'anonymat avec la signature de groupe ;

– Contrainte : Double certification ;

– Précondition : Authentification forte (étape 1 du procédé), choisir un serveur d'anonymat (SA) ;

– Objectifs : S'authentifier pour participer à une vente aux enchères tout en étant anonyme ;

– Acteur principal : Visiteur et SA;

– Scénario typique : M.Dupond est toujours décidé à participer à la vente aux enchères pour une œuvre d'art dont le prix de départ est 500.000 euros. Il souhaite rester anonyme pour cette vente afin de ne pas révéler ses moyens financiers ni son intérêt pour le type d'œuvre à vendre, et, s'il gagne l'enchère, il ne veut pas que l'on sache qu'il devient le nouveau propriétaire. Rester anonyme tout en signant est rendu possible grâce à la signature de groupe. M.Dupond fait donc appel aux services d'une autorité de certification délivrant une signature de groupe. Il s'inscrit à un groupe qui vérifie son identité avant de lui

fournir les moyens de créer ses clés et de l'enregistrer comme membre certifié. Un tel processus est schématisé figure 11.

2.4 Demande de participation avec certificat et autorisation

Cette fonction est schématisée figure 12.

- Phase du déroulement : Enchère ; elle fait partie de la troisième étape du procédé;
- Niveau de sécurité : Certificat et applet signée de génération de jetons d'enchères;
- Précondition : Pour le client, avoir un certificat, avoir choisi un article, autoriser le chargement des applets signées; pour le serveur d'enchères, avoir obtenu les moyens de vérifier une authentification anonyme (deuxième étape du procédé);
- Objectifs : Participer à une vente aux enchères ;
- Acteur principal : Client ;
- Scénario typique : Afin de participer à l'enchère, M.Dupond présente sa demande à l'aide d'un jeton signé. Ce premier jeton, noté W1000 pour M.Dupond et X1000 pour un autre client (voir figure 13), sert d'initialisation et de preuve pour la suite de la vente. Ce premier jeton est généré et signé par le client avec sa clé privée grâce à une applet transmise par le site d'enchère. Le jeton est associé aux paramètres de la vente, identifiant de l'article, prix actuel et valeur du pas. Pour M.Dupond, la signature est anonyme grâce à la signature de groupe.

2.5 Participation à une vente aux enchères

Cette fonction est schématisée figure 14.

- Phase du déroulement : Enchère ; elle fait partie de la troisième étape du procédé;
- Niveau de sécurité : Le jeton assure l'authenticité, l'intégrité et la confidentialité de l'ordre d'enchère ;
- Précondition : Etre inscrit à la vente, le jeton possède une filiation ;
- Objectifs : Soumettre un ordre d'enchère pour remporter la vente ;

– Acteur principal : Client ;

– Scénario typique : M.Martin participe à la vente aux enchères de la photographie qu'il a choisi avec un prix de départ à 600 euros et un pas à 10 euros. Il est le premier enchérisseur et il s'engage à enchérir à 610 euros en transmettant un jeton (W999). Au cours de l'enchère, un deuxième client augmente le prix à 620 euros. M.Martin est prêt à mettre plus et clique sur le bouton pour surenchérir à 630 euros. Il transmet alors le jeton d'indice 997, noté W997. En effet, comme décrit précédemment, chaque jeton correspond à une valeur calculée en fonction du prix de départ et du pas de l'enchère.

Dans cette vente, l'indice 999 représente la valeur 610 euros, 998-620, 997-630, 996-640, ... ;

Un tel processus est schématisé figure 15.

2.6 Traitement des ordres d'enchères

Cette fonction est schématisé figure 16.

– Phase du déroulement : Enchère ; elle fait partie de la troisième étape du procédé;

– Niveau de sécurité : Le jeton assure l'authenticité du client et l'intégrité des données ;

– Précondition : Avoir un jeton d'initialisation pour les enchères d'un client particulier sur un article ;

– Objectifs : Comparer les ordres d'enchères, enregistrer les ordres et informer de l'évolution des enchères ;

– Acteur principal : Client ;

– Scénario typique : Lorsque M.Martin clique sur le bouton pour enchérir, un jeton correspondant au prix est envoyé au serveur d'enchères. Côté serveur, le jeton permet de retrouver les informations nécessaires à l'ordre d'enchère, c'est-à-dire sa valeur, son propriétaire (M.Martin) et l'article visé. Pour connaître la position de M.Martin, son ordre est comparé aux ordres des autres clients. La proposition de M.Martin est enregistrée et le prix de la photo est actualisé.

Ce processus est schématisé figure 17.

2.7 Conclusion de la vente

Cette fonction est schématisé figure 18.

– Phase du déroulement : Conclusion de la vente ; elle comporte la quatrième étape du procédé;

– Niveau de sécurité : Identifier le gagnant et lever l'anonymat du gagnant en cas de signature de groupe ;

– Objectifs : Déterminer un gagnant et clore la transaction ;

– Acteur principal : Client, Vendeur, SA, Tiers de confiance ;

– Scénario typique : Le temps de la vente écoulé, le système détermine si M.Dupond a gagné ou non l'enchère en comparant les différentes propositions. L'offre de 800.000 euros est la plus forte et M.Dupond (anonyme) remporte l'œuvre d'art. Les autres clients sont prévenus qu'ils ont perdu. Le vendeur est informé que son article a trouvé un acheteur. Le Tiers de Confiance est alors chargé de lever l'anonymat de M.Dupond et de clore la transaction en tant qu'intermédiaire entre M.Dupond et le vendeur. Ce processus est schématisé figure 19.

2.8 Remarques

– Inscription pour la participation à une vente : L'inscription à une vente est liée à une session. Il est donc nécessaire de réinitialiser l'inscription en cas de déconnexion ou de changement de session ;

– Usage des certificats : Les certificats d'authentification forte et les certificats anonymes sont multi-usages. Il est donc possible d'utiliser un certificat pour plusieurs ventes sans avoir à renouveler les demandes à chaque vente, sauf en cas de révocation ou d'expiration du certificat;

– Propriétés à la demande du certificat anonyme : Lors de la connexion entre un client et le site serveur d'anonymat, la confidentialité et l'intégrité des informations transmises et la garantie d'anonymat du client vis-à-vis de l'extérieur sont assurées par un protocole de communication par exemple SSL ;

– Anticipation pour une première participation : La configuration de l'environnement technique du poste client (applet cryptographique signée) et les démarches d'obtention de certificats réclament une préparation à la participation à une vente.

3 Spécification de l'application d'enchères

Cette partie décrit succinctement l'API pour les services de l'application aux niveaux suivants :

- Demande d'un certificat anonyme et de participation à une vente;
- Contrôle de demande de participation;
- Enchère;
- Vérification d'enchère;
- Conclusion de la vente.

Les étapes indiquées par une * sont considérées comme basiques dans le cadre du procédé conforme à l'invention.

3.1 Demande d'un certificat anonyme et de participation à une vente

- S'authentifier de manière forte auprès de l'ACA*
- Générer les clés*
- Envoyer la clé publique à l'ACA*
- Obtenir un certificat anonyme auprès de l'ACA*
- Générer les jetons*
- Stocker les jetons*
- Signer le jeton d'initialisation et l'id article*
- Transmettre le jeton signé, le certificat et l'id article signé*
- Recevoir la confirmation
- Afficher la confirmation

3.2 Contrôle de demande de participation

- Récupérer les moyens de vérifier une authentification anonyme auprès de l'ACA*
- Recevoir les données de l'applet
- Vérifier la signature avec les moyens de l'ACA*
- Se connecter à la base de données
- Enregistrer les données jeton, certificat, id article
- Sélectionner dans la base le prix max de l'article
- Transmettre la confirmation

3.3 Enchère

– Actualiser le prix max

– Calculer le jeton par rapport au prix supérieur

W_i ?

prixsup = prixmax + pas

j = (prixsup - prixdedepart)/pas

i = nombretotaldejetons - j

– Transmettre le jeton*

– Recevoir la réponse

3.4 Vérification d'enchère

– Décompter le temps de la vente

– Recevoir le jeton (W_i)*

– Vérifier le jeton (trouver dans la base W_k tel que $h^{i}(W_i) = W_k$)*

– Sélectionner les données de la base pour W_k

– Sélectionner le prix max de l'id article

– Calculer le prix correspondant au jeton reçu W_i

prix de W_i = prix de W_k +(i* pas)

– Comparer le prix max au prix de Wi

– Enregistrer le prix de W_i (UPDATE)

– Répondre au client sur sa situation

3.5 Conclusion de la vente

– Détecter la fin de l'enchère

– Déterminer l'offre la plus haute

– Lever l'anonymat*

– Informer l'acheteur gagnant

– Informer le vendeur

<u>4 Organisation technique</u>

4.1 Architecture client – serveur

Cette architecture est schématisée figure 20.

On y retrouve un navigateur Client, un Serveur ACA et un Serveur Se enchères (ces derniers étant chacun associé à une base de données spécifiques) aptes à mettre en oeuvre les étapes précitées.

4.2 Outils de prototypage : Base de données, serveur d'application et Plug-in Java

La base de données utilisée par les inventeurs pour un prototypage de cette application est une base Oracle 8i. Oracle est un SGBD (système de gestion de bases de données) relationnel édité par la société du même nom. Oracle dispose d'un langage permettant la définition et la manipulation des données : le langage SQL (Structured Query Language), qui est devenu le langage normalisé dans le domaine des bases de données relationnelles. SQL*PLUS est l'interface utilisateur d'Oracle qui permet d'utiliser interactivement le langage SQL sur une instance Oracle.

Le langage de programmation et les technologies utilisées pour l'implantation sont Java. L'application est gérée par le produit d'IBM WebSphere 3.5. WebSphere Application Server permet de réaliser des transactions et des interactions Web. Il fournit une plate-forme portable de déploiement d'applications Web Java, axée sur la prise en charge et l'exécution de servlets, de JavaBeans et de fichiers Java Server Pages (JSP). C'est une interface avec le serveur Web pour gérer les requêtes client portant sur les ressources côté serveur et pour les acheminer vers le serveur d'applications en vue de leur traitement. L'outil utilisé dans WebSphere est le moteur de servlet. Il s'exécute à l'intérieur du serveur d'applications et gère les requêtes relatives aux servlets, aux fichiers Java Server Pages (JSP) et aux applications Web qui les contiennent.

Le poste client a été testé sur un système Windows avec le Plug-in Java. Le Plug-in (fournit par Sun) permet d'actualiser la version de la JVM du navigateur (IE ou Netscape). Le Java-plugin remplace le Java Runtime par défaut du navigateur par le JRE de Sun.

Bien entendu la présente invention n'est pas limitée au mode de réalisation particulier qui vient d'être décrit mais s'étend à toute variante conforme à son esprit.

REFERENCES

[1] G. Ateniese, J. Camenisch, M. Joye, G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In L. Bellare, editor, Advances in Cryptology – Crypto 2000, volume 1880 of LNCS, pages 255-270. Springer-Verlag, 2000.

[2] S. Canard, M Girault. Implementing group signature schemes with smart cards. conférence CARDIS 2002.

[3] J. Camenisch, M. Michels. A group signature scheme based on an RSA-variant. Proceedings of Eurocrypt'98, volume 1514 of LNCS. Springer-Verlag, 1998.

[4] J. Camenisch, M. Stadler. Efficient group signature schemes for large groups. Proceedings of Crypto'97, volume 1296 of LNCS, pages 410-424. Springer-Verlag, 1997.

[5] K.Q. Nguyen, J. Traoré. "An Online Public Auction Protocol Protecting Bidder Privacy". Information Security and Privacy, 5th Australasian Conference-ACISP 2000, pages 427-442. Springer-Verlag, 2000.

[6] J Camenisch, U. Maurer, M. Stadler. Digital payment systems with passive anonymity-revoking trustees. Proceedings of ESORICS'96, volume 1146 of LNCS, pages 33-43. Springer-Verlag, 1996.

[7] J Camenisch, U. Maurer, M. Stadler. Digital payment systems with passive anonymity-revoking trustees. Journal of Computer Security, vol. 5, number 1, IOS Press, 1997.

[8] A. de Solages, J. Traoré. An Efficient fair off-line electronic cash system with extensions to checks and wallet with observers, Proceedings of Financial Crypto'98, volume 1465 of LNCS, pages 275-295. Springer-Verlag, 1998.

[9] A. de Solages et J. Traoré, Procédé de signature numérique juste, n° 98 02197, CNET/02959, dépôt du 24/02/98.

[10] Y. Frankel, Y. Tsiounis, M. Yung. Indirect discourse proofs: achieving fair off-line electronic cash. Proceedings of Asiacrypt'96, volume 1136 of LNCS, pages 244-251. Springer-Verlag, 1996.

[11] Y. Frankel, Y. Tsiounis et M. Yung . "Fair off-line cash made easy". Proceedings of Asiacrypt'98, volume 1514 of LNCS. Springer-Verlag, 1998.

[12] KOBAYASHI K ; MORITA H : "Efficient sealed-bid auction by using one-way functions", IEICE Transactions on fundamentals of electronics, communications and computer sciences, institute of

electronics information and comm. eng., vol. e84-A, n° 1, 1 janvier 2001 (2001-01-01), pages 289-294.

[13] SUZUKI K ; KOBAYASHI K ; MORITA H : "Efficient sealed-bid auction using hash chain", Information security and cryptology - ICISC 2000. Third international conference. Proceedings (lecture notes in computer science, vol. 2015, Springer verlag), 9 décembre 2000 (2000-12-09), pages 183-191.

[14] BYOUNGCHEON LEE ; KWANGJO KIM ; JOONGSOO MA : "Efficient public auction wih one-time registration and public verifiability", Indocrypt 2001, second international conference on cryptology in India, 16-20 décembre 2001, pages 162-174.

REVENDICATIONS

1. Procédé d'accès à un service avec authentification rapide et anonymat révocable, caractérisé par le fait qu'il comprend les étapes consistant à :

i) identifier et enregistrer un Client (C) et lui fournir des moyens lui permettant de s'authentifier auprès d'une Autorité de Certification Anonyme (ACA),

ii) authentifier le Client auprès de l' Autorité de Certification Anonyme sur la base des moyens fournis en i) et fournir des moyens lui permettant de s'authentifier de manière anonyme auprès d'un Serveur (Se),

iii) authentifier le Client par la production d'une signature anonyme et ouvrir et maintenir une session d'authentification anonyme auprès d'un Serveur (Se), et

iv) permettre sélectivement un contact entre le Serveur (Se) et l'Autorité de Certification Anonyme (ACA) pour lever l'anonymat du Client (C) sur la base de la signature fournie à l'étape iii).

2. Procédé selon la revendication 1, caractérisé par le fait qu'il comprend une étape additionnelle d'échange entre l'Autorité de Certification Anonyme (ACA) et le Serveur (Se) préalable à l'étape ii) par laquelle le Serveur (Se) présente à ladite Autorité (ACA) une requête d'obtention de moyens permettant de vérifier l'authentification anonyme fournie par un Client (C).

3. Procédé selon l'une des revendications 1 ou 2, caractérisé par le fait que l'étape iii) comprend trois phases :

. une première phase dans laquelle le Client (C) calcule un ensemble de données, formé d'une suite de jetons, l'un de ceux-ci permettant d'ouvrir une session, tandis que les autres permettent de la maintenir,

. une deuxième phase dans laquelle le Client (C) s'engage fortement sur la suite de jetons auprès du Serveur, et

. une troisième phase de maintien de la session à l'aide de la suite de jetons.

4. Procédé selon la revendication 3, caractérisé par le fait que tous les jetons sont à usage unique et fortement dépendants les uns des autres.

5. Procédé selon l'une des revendications 3 ou 4, caractérisé par le fait que l'étape de génération des jetons met en oeuvre deux primitives cryptographiques : une fonction de hachage et un nombre aléatoire.

6. Procédé selon la revendication 5, caractérisé par le fait que le premier jeton est obtenu en appliquant la fonction de hachage au nombre aléatoire, le deuxième jeton est obtenu en appliquant à nouveau la fonction de hachage au premier jeton obtenu, et ainsi de suite pour obtenir n jetons : $H(W_0)=W_1$; $H(W_{n-1})=W_n$.

7. Procédé selon l'une des revendications 3 à 6, caractérisé par le fait que la deuxième phase comprend l'obtention d'une signature anonyme d'un jeton d'initialisation W_n permettant l'authentification d'un Client par le Serveur.

8. Procédé selon l'une des revendications 3 à 7, caractérisé par le fait que des informations, telles qu'une valeur numéraire, sont associées au jeton d'initialisation.

9. Procédé selon l'une des revendications 3 à 8, caractérisé par le fait qu'à chaque nouvelle authentification le Client (C) transmet au Serveur (Se) un jeton de rang inférieur d'au moins une unité à celui précédemment utilisé.

10. Procédé selon l'une des revendications 3 à 9, caractérisé par le fait qu'à chaque nouvelle authentification le Client (C) transmet au Serveur (Se) un jeton W_i dont le rang i est choisi représentatif de la valeur d'une opération, par exemple du nombre de pas d'une enchère.

11. Procédé selon l'une des revendications 1 à 10, caractérisé par le fait qu'il est appliqué à des enchères et que les étapes de surenchérissement par le Client (C) sont opérées par envois successifs de jetons de rang inférieur.

12. Procédé selon l'une des revendications 1 à 11, caractérisé par le fait qu'il met en oeuvre une signature de groupe, par association

de plusieurs identifiants et clés privées respectives, à une unique clé publique de groupe.

13. Procédé selon l'une des revendications 1 à 12, caractérisé par le fait qu'il met en oeuvre une signature aveugle.

14. Procédé selon l'une des revendications 12 et 13, caractérisé par le fait que les pouvoirs de levée d'anonymat sont répartis entre au moins deux autorités.

15. Système apte à permettre l'ouverture et le maintien d'une session d'authentification garantissant la non répudiation, caractérisé par le fait qu'il comprend des moyens adaptés pour la mise en œuvre de trois phases :

. une première phase dans laquelle un Client (C) calcule un ensemble de données, formé d'une suite de jetons, l'un de ceux-ci permettant d'ouvrir une session, tandis que les autres permettent de la maintenir,

. une deuxième phase dans laquelle le Client s'engage fortement sur la suite de jetons auprès d'un Serveur (se), et

. une troisième phase de maintien de la session à l'aide de la suite de jetons.

16. Système selon la revendication 15, caractérisé par le fait que l'étape de génération des jetons met en oeuvre deux primitives cryptographiques : une fonction de hachage et un nombre aléatoire.

17. Système selon l'une des revendications 15 à 16, caractérisé par le fait qu'il met en oeuvre une signature de groupe, par association de plusieurs identifiants et clés privées respectives, à une unique clé publique de groupe.

18. Système selon l'une des revendications 15 à 17, caractérisé par le fait qu'il met en oeuvre une signature aveugle.

19. Système selon l'une des revendications 15 à 18, caractérisé par le fait que les pouvoirs de levée d'anonymat sont répartis entre au moins deux autorités.

FIG.1

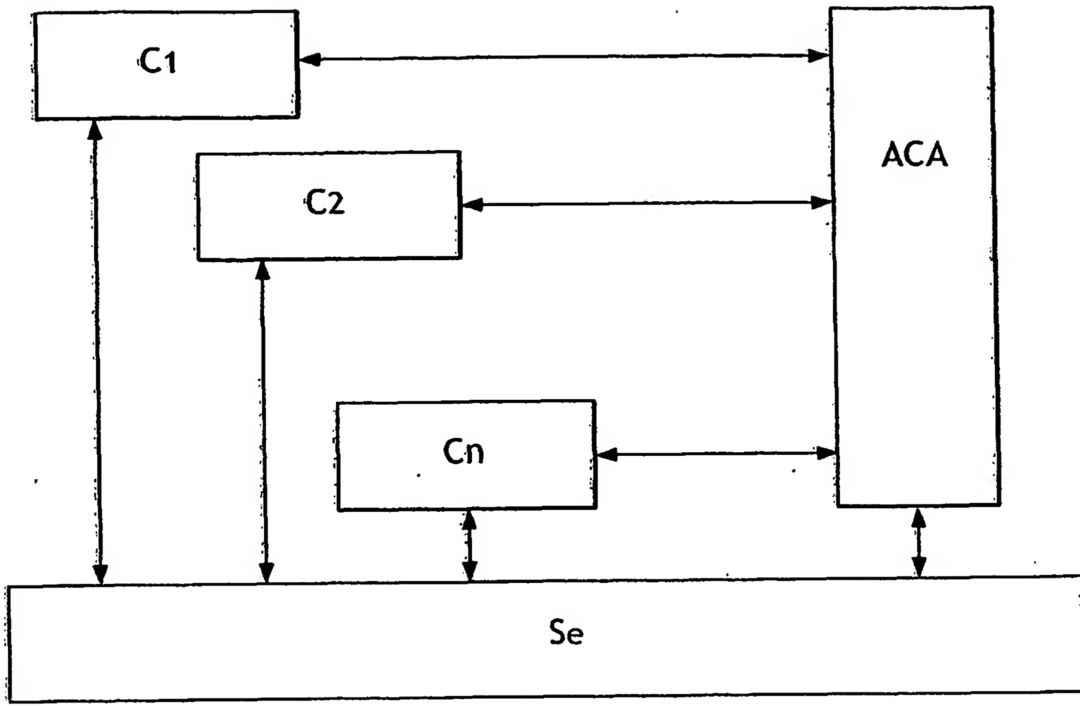

C1
C2
Cn
ACA
Se

FIG.2

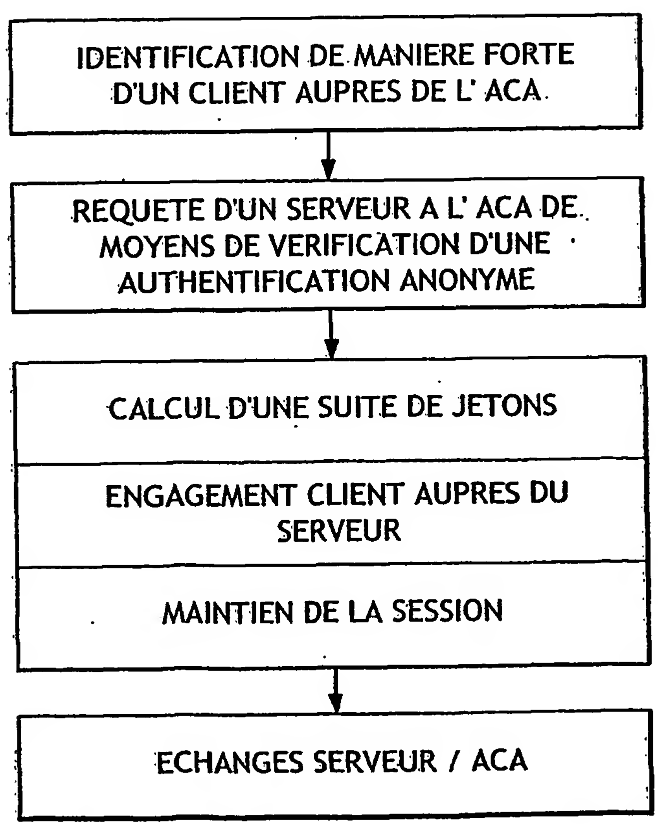

IDENTIFICATION DE MANIERE FORTE D'UN CLIENT AUPRES DE L' ACA
REQUETE D'UN SERVEUR A L' ACA DE MOYENS DE VERIFICATION D'UNE AUTHENTIFICATION ANONYME
CALCUL D'UNE SUITE DE JETONS
ENGAGEMENT CLIENT AUPRES DU SERVEUR
MAINTIEN DE LA SESSION
ECHANGES SERVEUR / ACA

FIG.3

Protocole de signature du jeton d'initialisation et d'ouverture de session

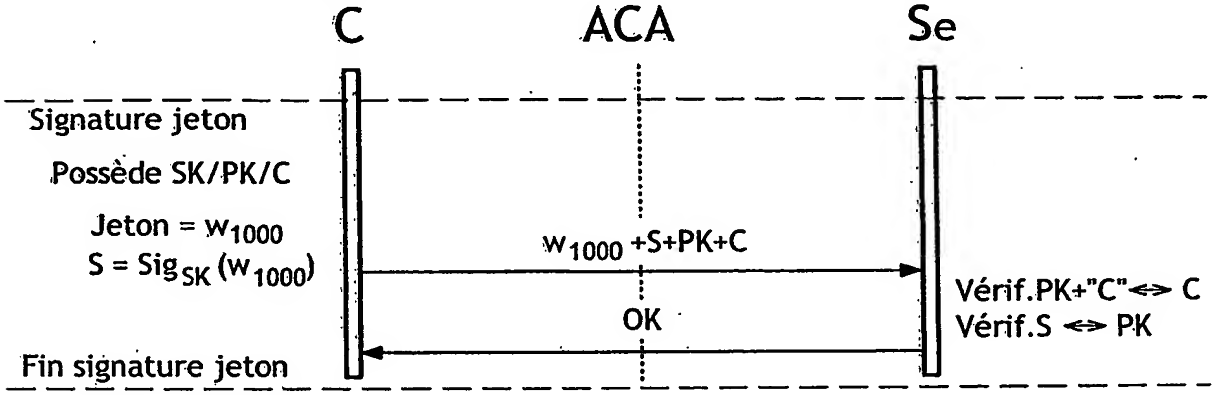


FIG.4

Certificat Anonyme

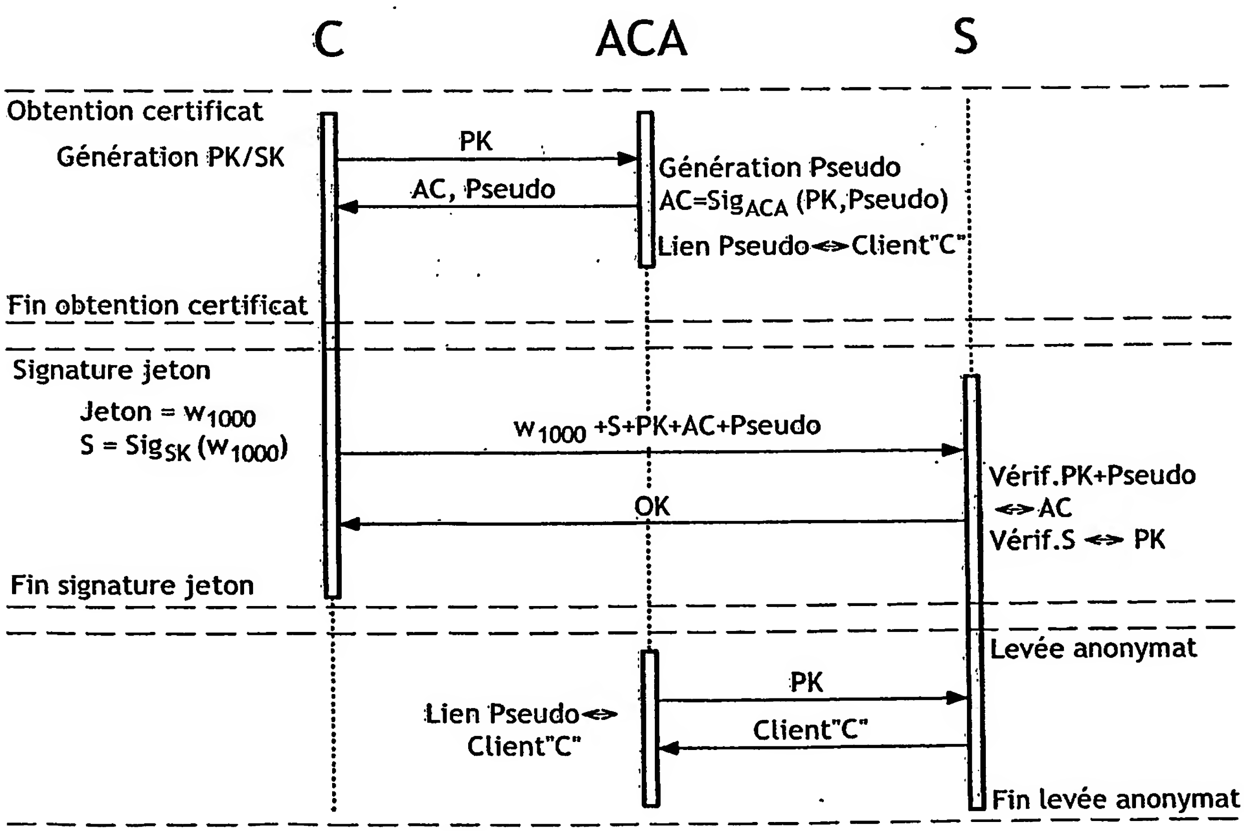


FIG.5

Signature aveugle à anonymat révocable

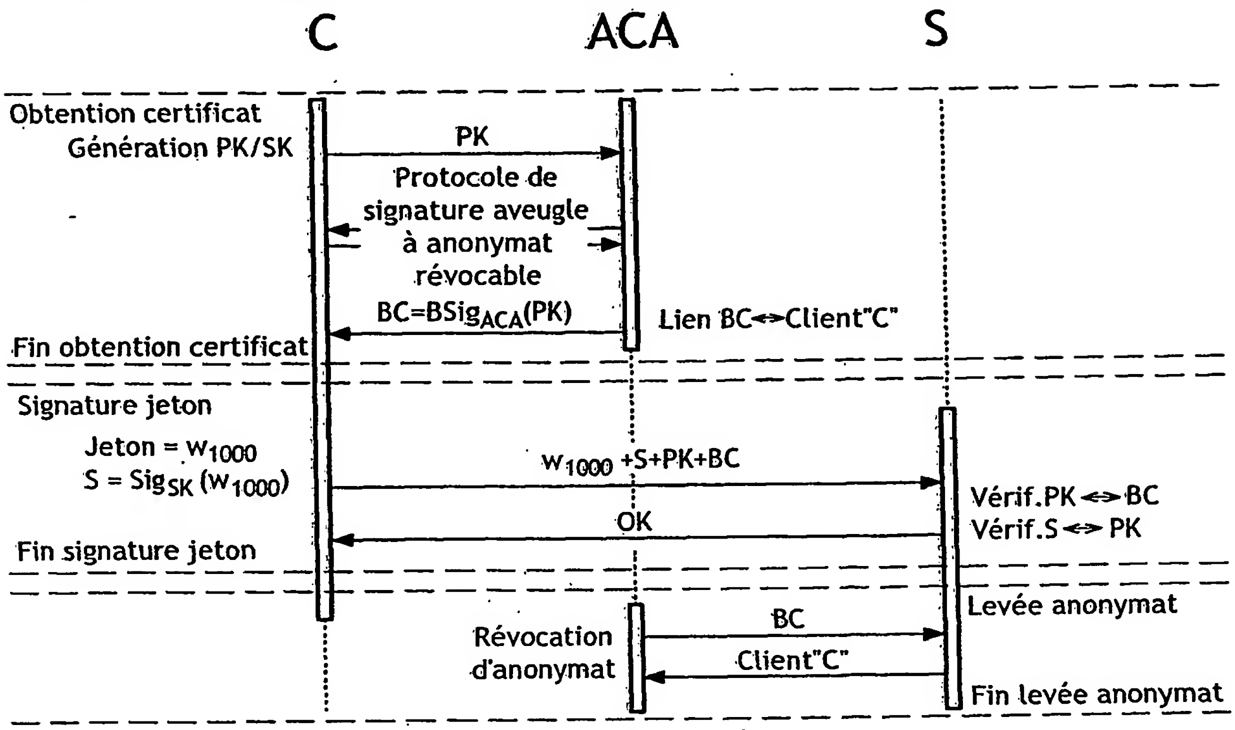


FIG.6

Signature de groupe

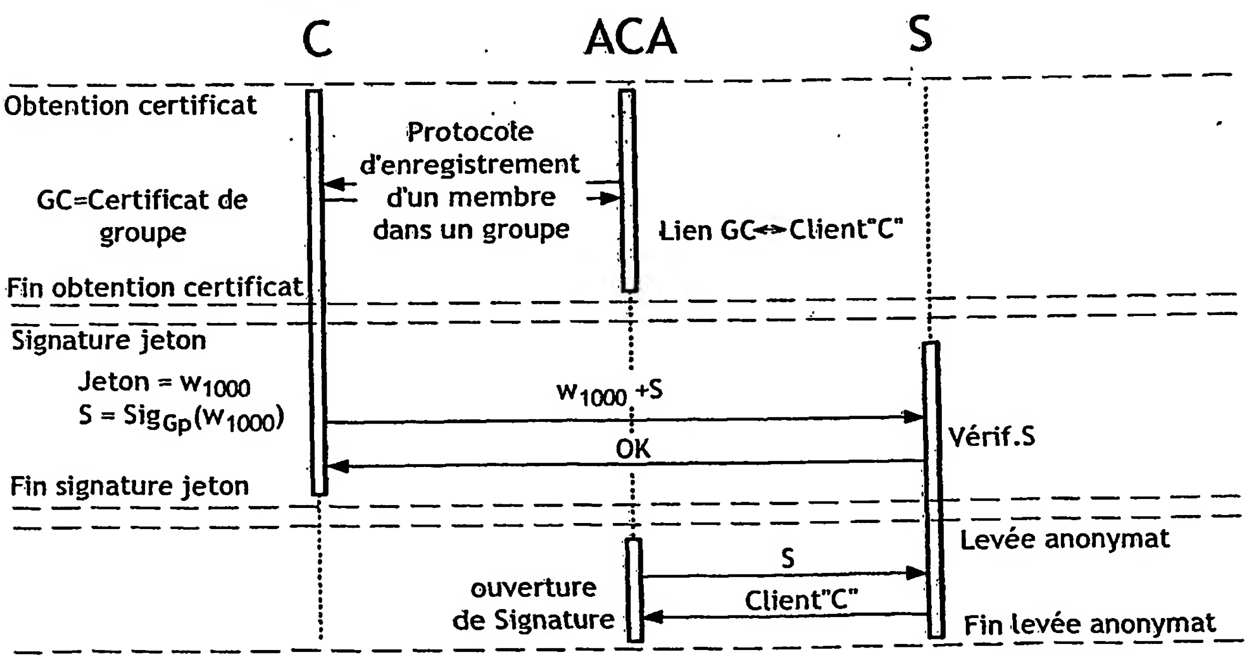


FIG.7

Serveur S : initialisation				
Client C1		Client C2		Prix
Jeton	Valeur	Jeton	Valeur	Prix départ
W_{1000}	signature	X_{1000}	signature	1000

Ordre 1 : Enchère client 1				
Client C1		Client C2		Prix
Jeton	Valeur	Jeton	Valeur	Prix actuel
W_{999}	100	X_{1000}	0	1100

Ordre 2 : Enchère client 1				
Client C1		Client C2		Prix
Jeton	Valeur	Jeton	Valeur	Prix actuel
W_{999}	100	X_{997}	3*100	1300

Ordre 3 : Enchère client 1				
Client C1		Client C2		Prix
Jeton	Valeur	Jeton	Valeur	Prix actuel
W_{996}	4*100	X_{997}	3*100	1400

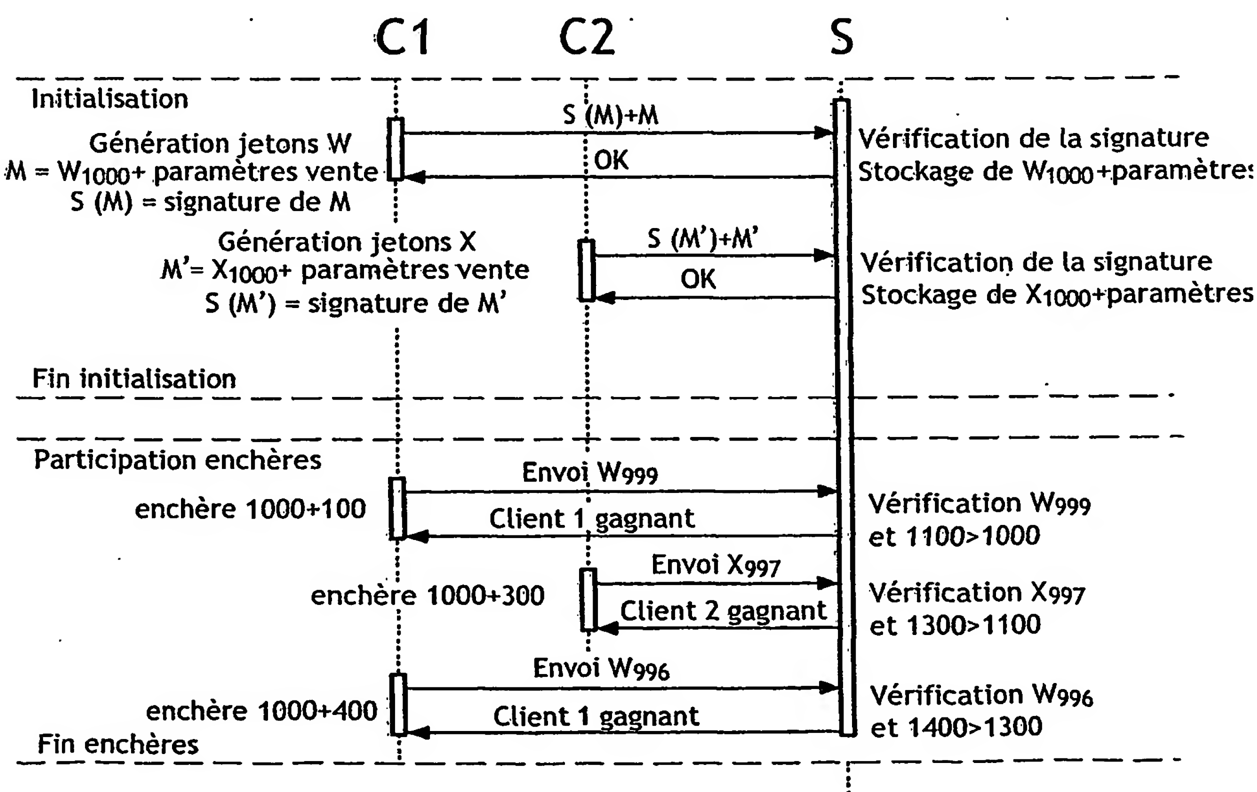


FIG.8

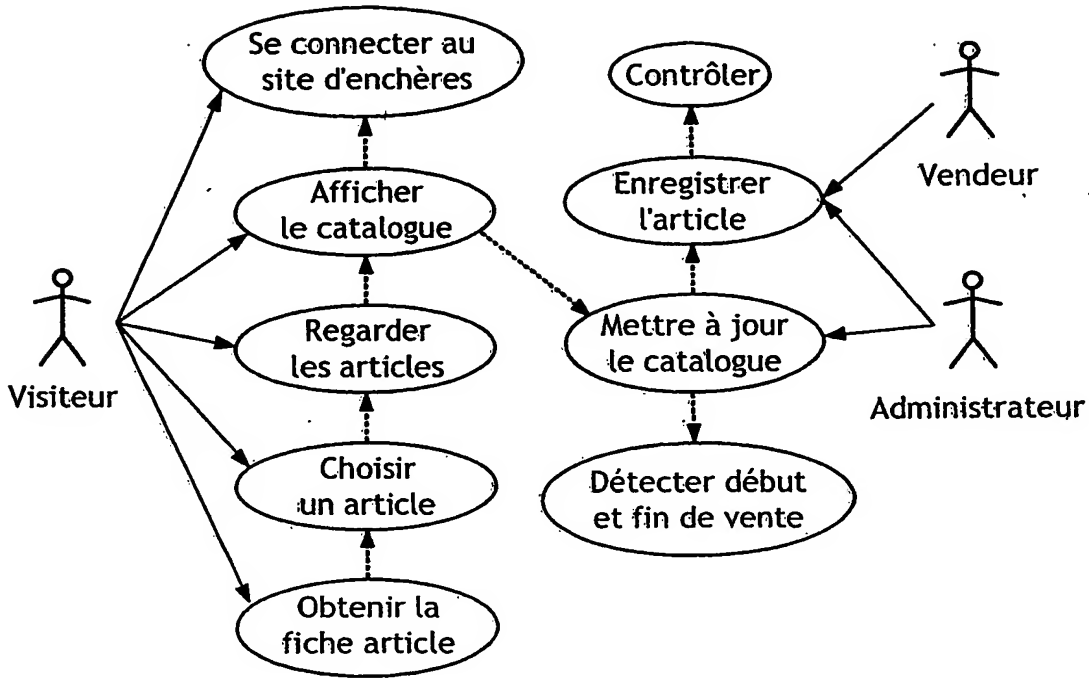

Se connecter au site d'enchères
Afficher le catalogue
Regarder les articles
Choisir un article
Obtenir la fiche article
Visiteur
Contrôler
Enregistrer l'article
Mettre à jour le catalogue
Détecter début et fin de vente
Vendeur
Administrateur

FIG.9

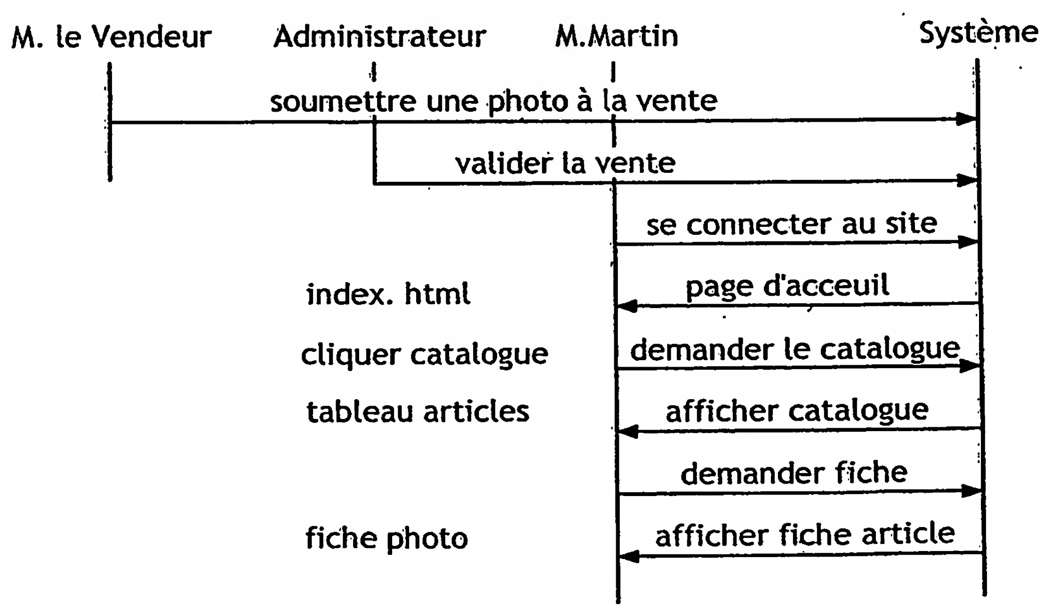

M. le Vendeur
Administrateur
M.Martin
Système
soumettre une photo à la vente
valider la vente
se connecter au site
index. html
page d'acceuil
cliquer catalogue
demander le catalogue
tableau articles
afficher catalogue
demander fiche
fiche photo
afficher fiche article

FIG.10

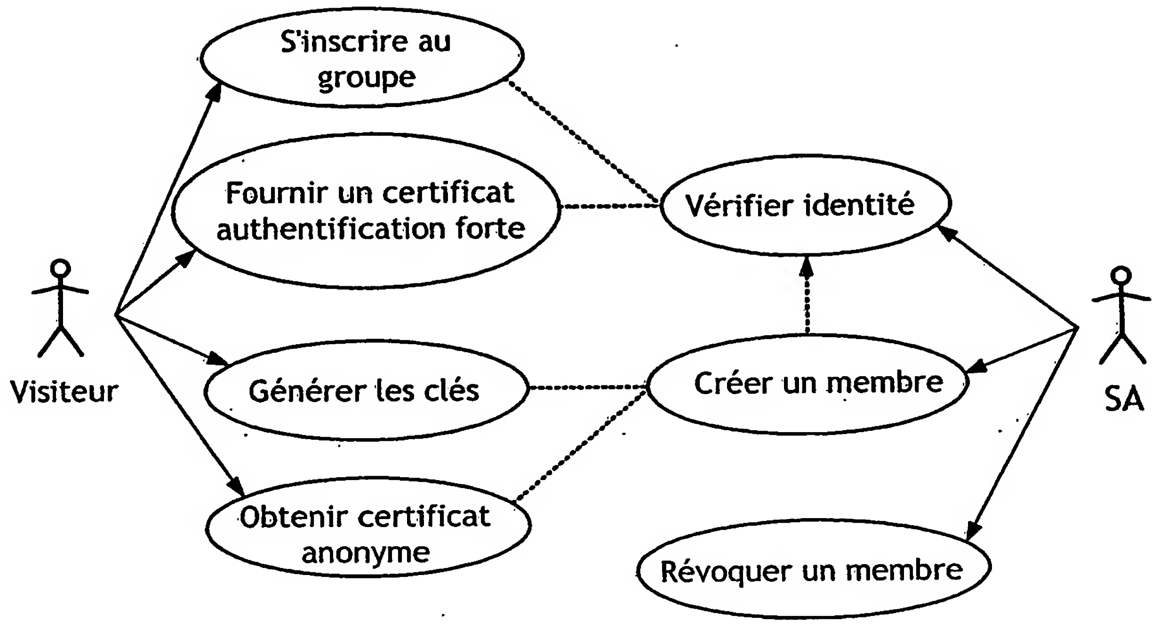

S'inscrire au groupe
Fournir un certificat authentification forte
Vérifier identité
Visiteur
Générer les clés
Créer un membre
SA
Obtenir certificat anonyme
Révoquer un membre

FIG.11

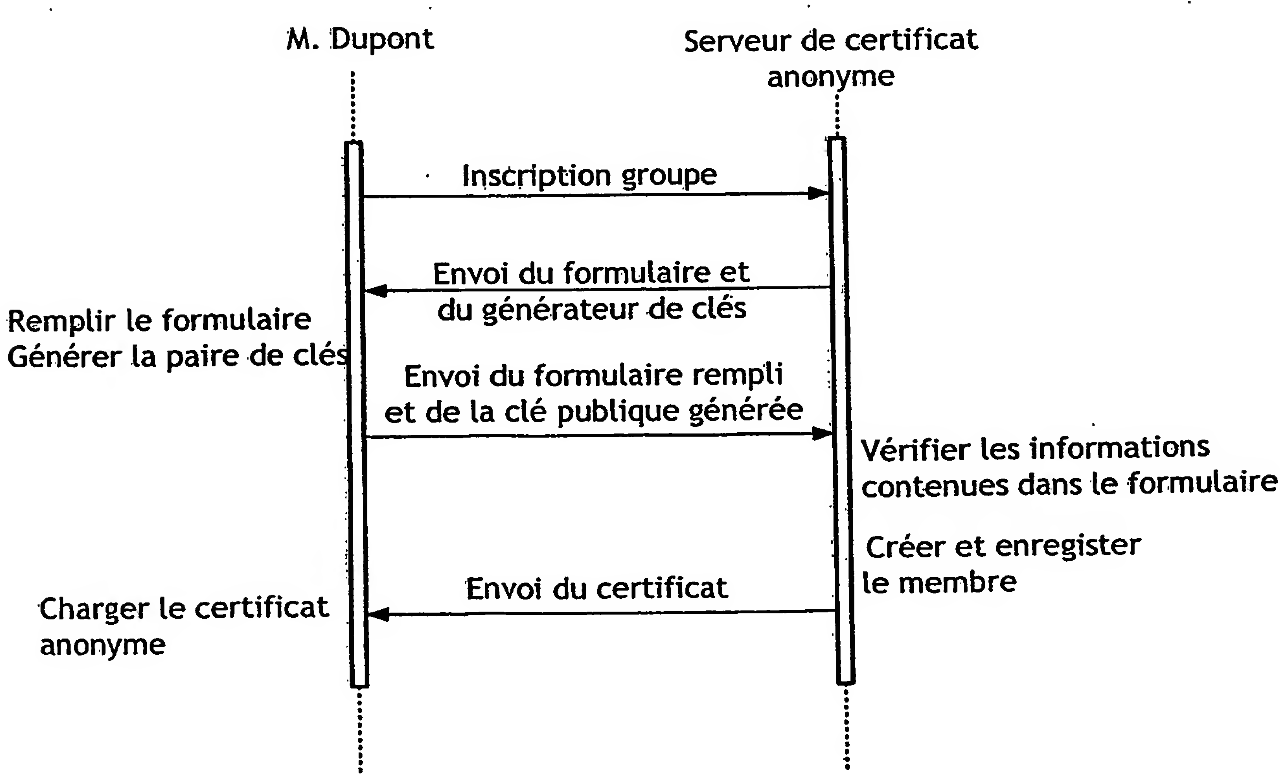

M. Dupont
Serveur de certificat anonyme
Inscription groupe
Envoi du formulaire et du générateur de clés
Remplir le formulaire
Générer la paire de clés
Envoi du formulaire rempli et de la clé publique générée
Vérifier les informations contenues dans le formulaire
Créer et enregistrer le membre
Envoi du certificat
Charger le certificat anonyme

FIG.12

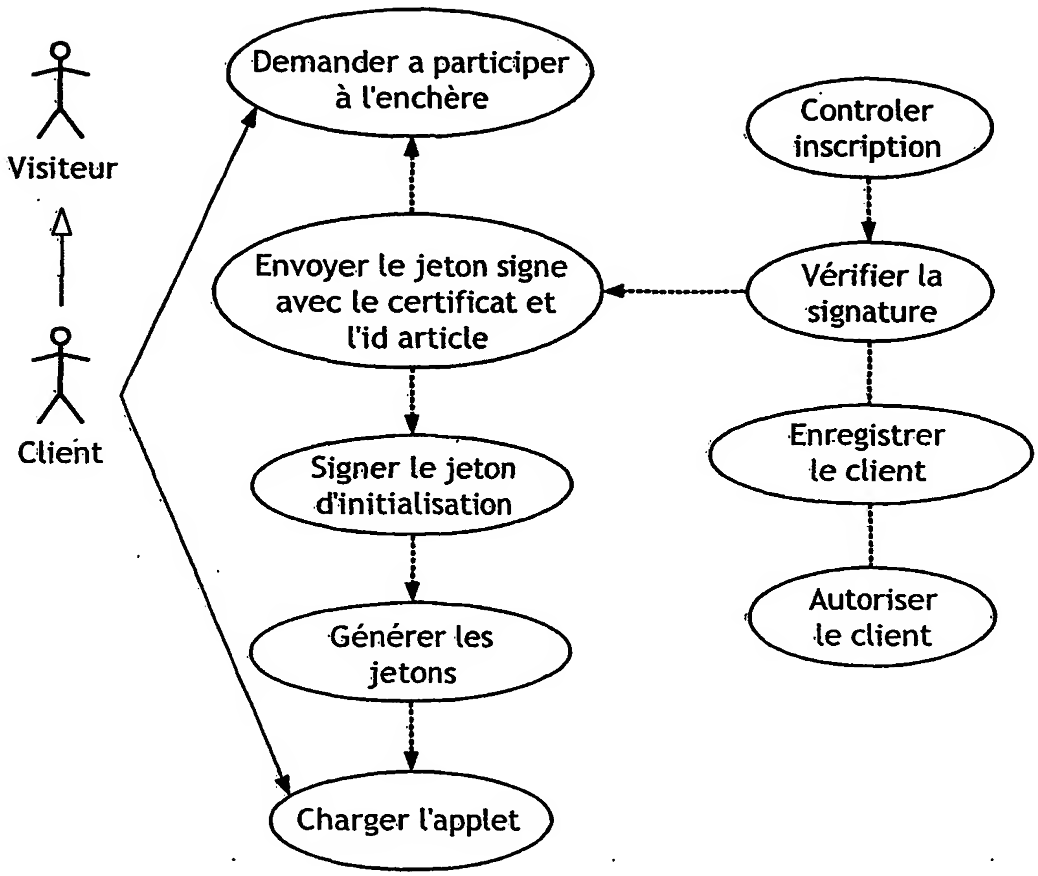

Visiteur
Client
Demander a participer à l'enchère
Envoyer le jeton signe avec le certificat et l'id article
Signer le jeton d'initialisation
Générer les jetons
Charger l'applet
Controler inscription
Vérifier la signature
Enregistrer le client
Autoriser le client

FIG.13

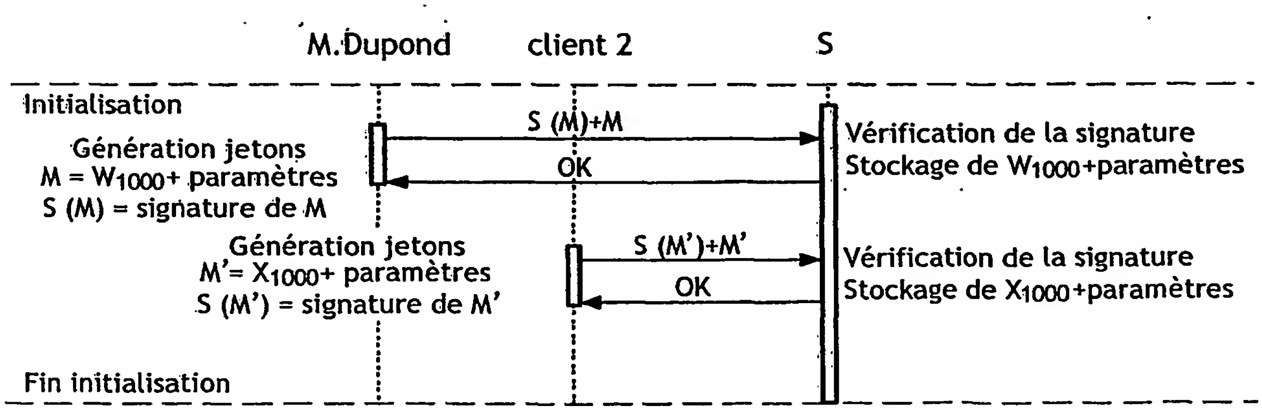

M. Dupond
client 2
S
Initialisation
Génération jetons
M = W1000+ paramètres
S (M) = signature de M
S (M)+M
OK
Vérification de la signature
Stockage de W1000+paramètres
Génération jetons
M'= X1000+ paramètres
S (M') = signature de M'
S (M')+M'
OK
Vérification de la signature
Stockage de X1000+paramètres
Fin initialisation

FIG.14

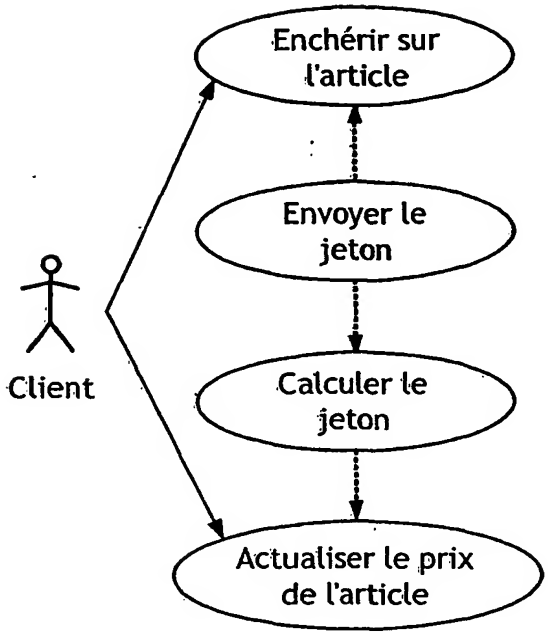

Enchérir sur l'article
Envoyer le jeton
Calculer le jeton
Actualiser le prix de l'article
Client

FIG.15

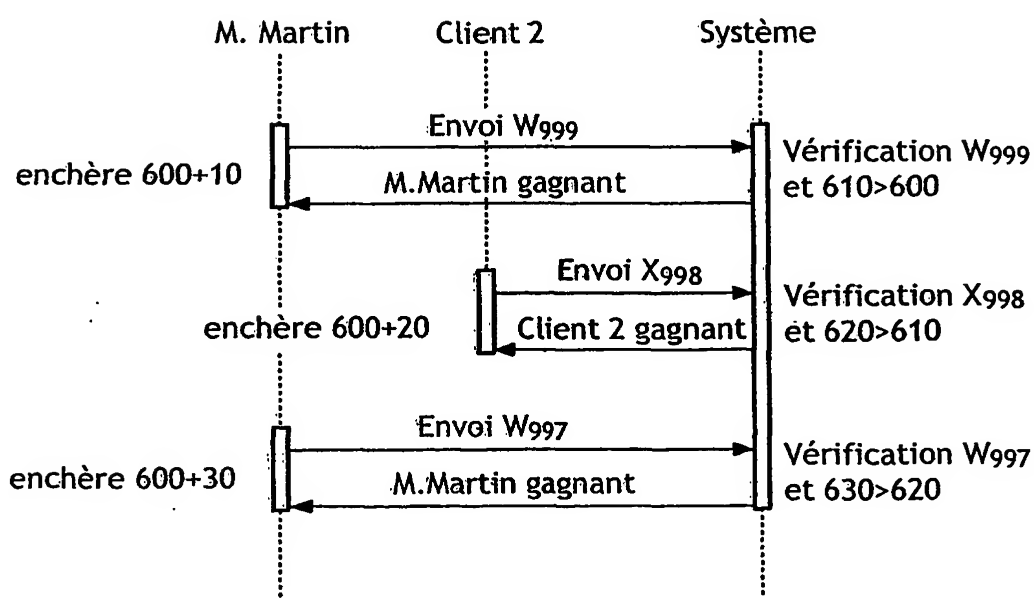

M. Martin
Client 2
Système
Envoi W999
enchère 600+10
M.Martin gagnant
Vérification W999 et 610>600
Envoi X998
enchère 600+20
Client 2 gagnant
Vérification X998 et 620>610
Envoi W997
enchère 600+30
M.Martin gagnant
Vérification W997 et 630>620

FIG.16

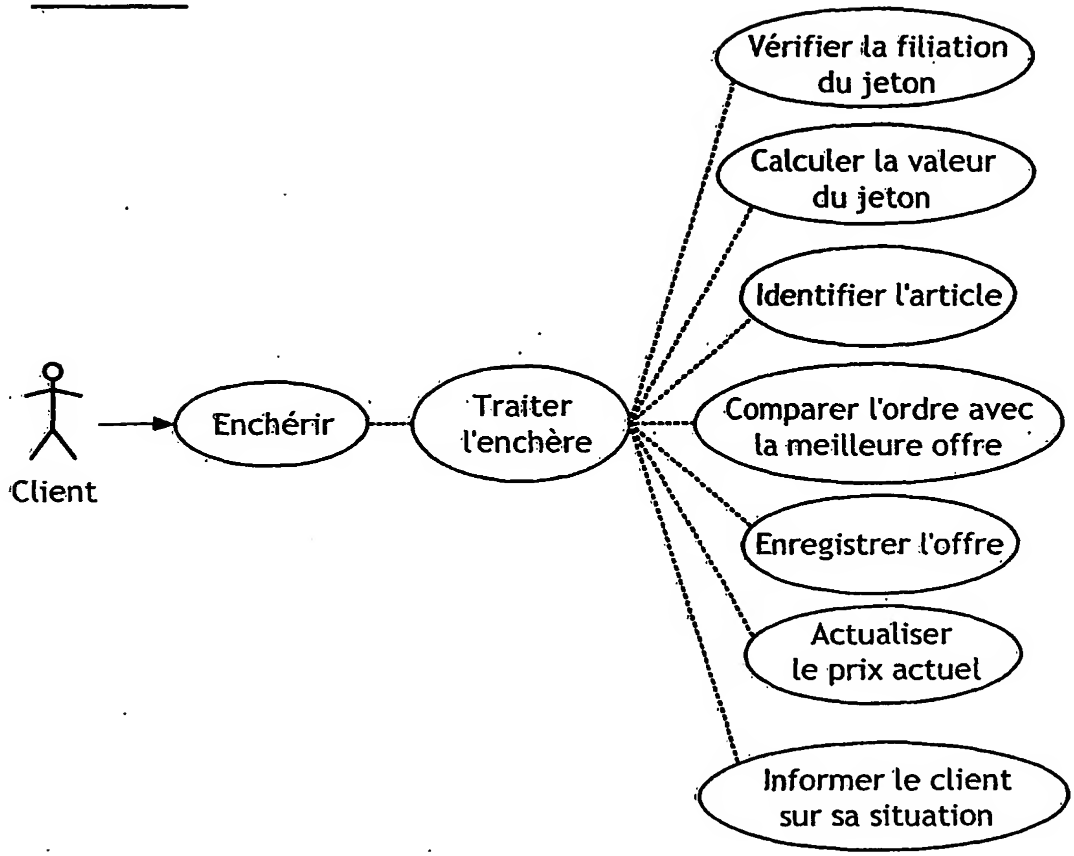

Vérifier la filiation du jeton
Calculer la valeur du jeton
Identifier l'article
Client
Enchérir
Traiter l'enchère
Comparer l'ordre avec la meilleure offre
Enregistrer l'offre
Actualiser le prix actuel
Informer le client sur sa situation

FIG.17

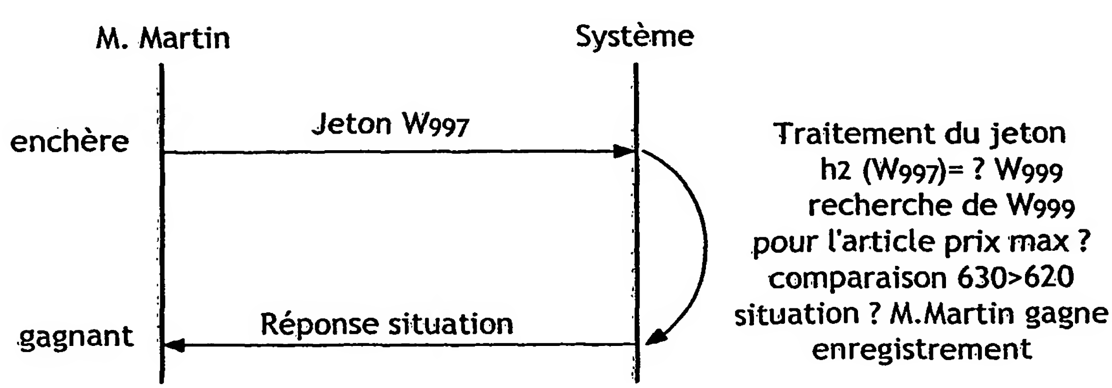

M. Martin
Système
enchère
Jeton W997
Traitement du jeton
h2 (W997)= ? W999
recherche de W999
pour l'article prix max ?
comparaison 630>620
situation ? M.Martin gagne
enregistrement
gagnant
Réponse situation

FIG.18

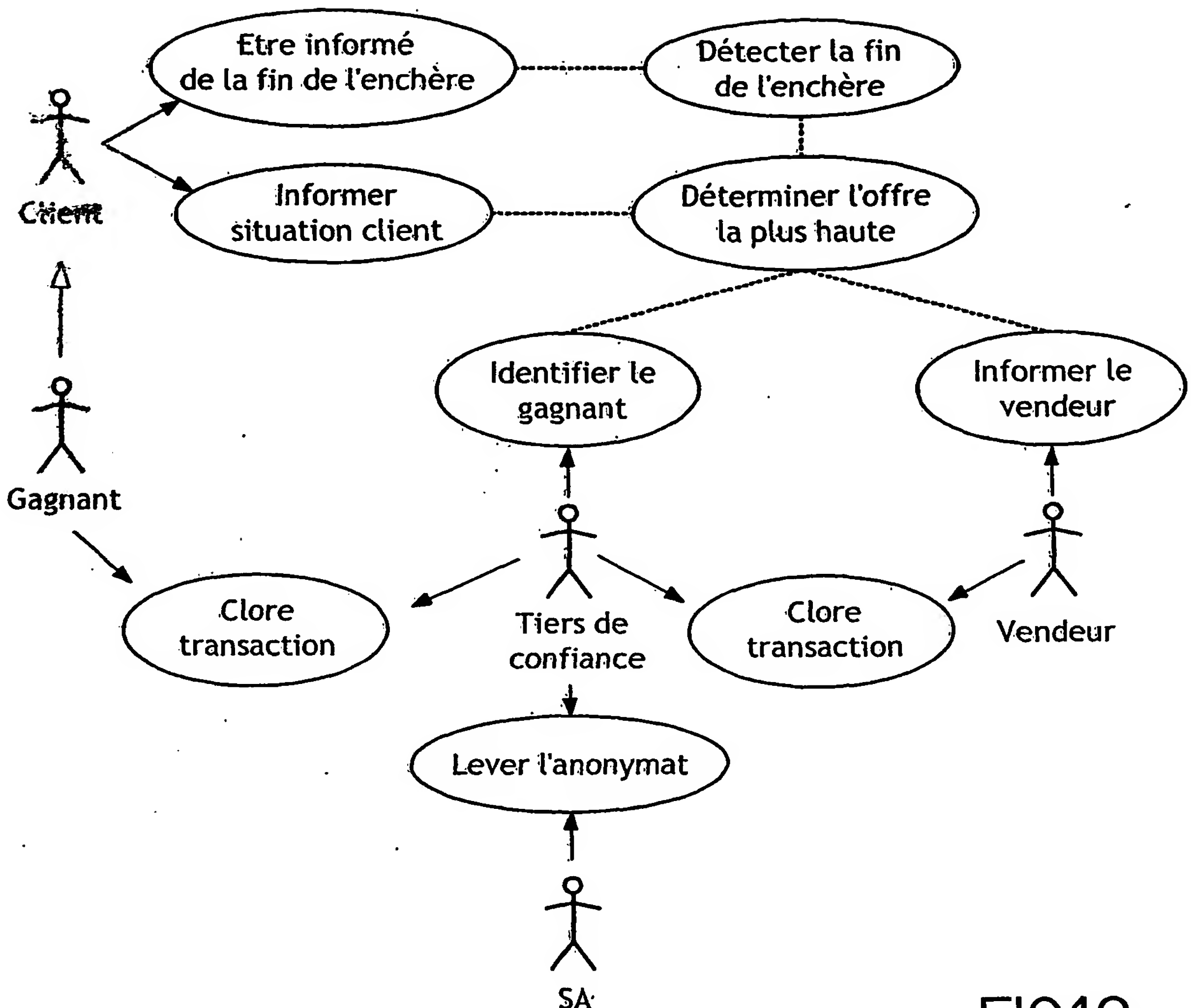

Etre informé de la fin de l'enchère
Détecter la fin de l'enchère
Client
Informer situation client
Déterminer l'offre la plus haute
Identifier le gagnant
Informer le vendeur
Gagnant
Clore transaction
Tiers de confiance
Clore transaction
Vendeur
Lever l'anonymat
SA

FIG.19

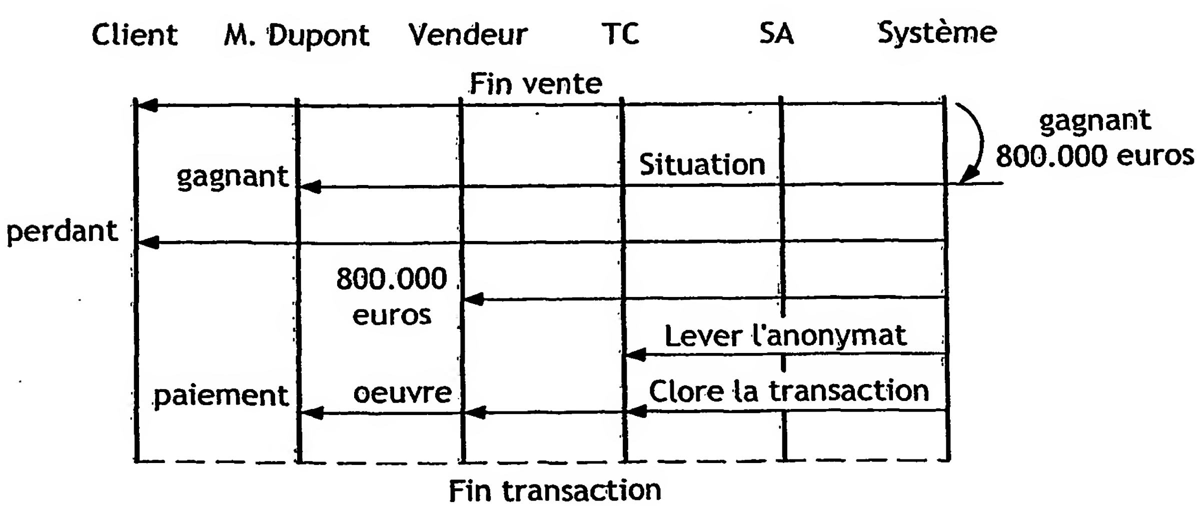
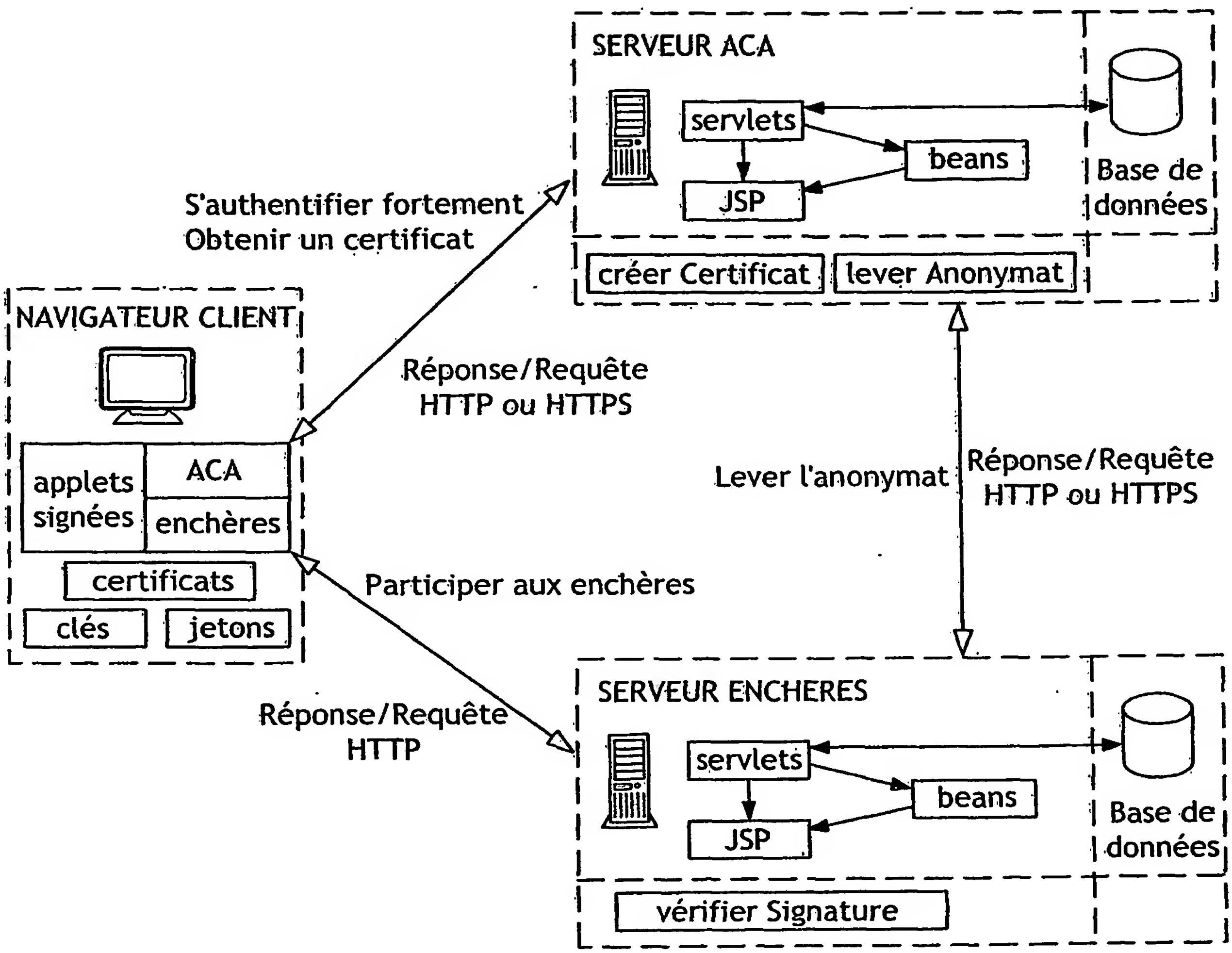

Client
M. Dupont
Vendeur
TC
SA
Système
Fin vente
gagnant 800.000 euros
Situation
gagnant
perdant
800.000 euros
Lever l'anonymat
Clore la transaction
paiement
oeuvre
Fin transaction

FIG.20


SERVEUR ACA
servlets
beans
JSP
Base de données
créer Certificat
lever Anonymat
S'authentifier fortement
Obtenir un certificat
NAVIGATEUR CLIENT
applets signées
ACA
enchères
certificats
clés
jetons
Réponse/Requête HTTP ou HTTPS
Lever l'anonymat
Réponse/Requête HTTP ou HTTPS
Participer aux enchères
Réponse/Requête HTTP
SERVEUR ENCHERES
servlets
beans
JSP
Base de données
vérifier Signature

INTERNATIONAL SEARCH REPORT

PCT/FR 03/03380

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KOBAYASHI K; MORITA H: "EFFICIENT SEALED-BID AUCTION BY USING ONE-WAY FUNCTIONS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. , vol. e84-A, no. 1, 1 January 2001 (2001-01-01), pages 289-294, XP001006551 TOKYO, JP page 289 page 291, left-hand column -page 293, left-hand column ---	1-19

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2004	07/05/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SUZUKI K ; KOBAYASHI K ; MORITA H : "Efficient sealed-bid auction using hash chain" INFORMATION SECURITY AND CRYPTOLOGY - ICISC 2000. THIRD INTERNATIONAL CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2015, SPRINGER VERLAG), 9 December 2000 (2000-12-09), pages 183-191, XP002247412 Seoul, South Korea ISBN: 3-540-41782-6 page 183 page 185 -page 189 ---	1-19
X	BYOUNGCHEON LEE; KWANGJO KIM; JOONGSOO MA: "Efficient Public Auction with One-Time Registration and Public Verifiability" INDOCRYPT 2001, SECOND INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, 'Online! 16 - 20 December 2001, pages 162-174, XP002247413 Indian Institute of Technology, Madras, Chennai, India Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/cs> 'retrieved on 2003-07-04! page 166 -page 172 ---	1-19
A	ZHANG N ET AL: "Anonymous public-key certificates for anonymous and fair document exchange" IEE PROCEEDINGS: COMMUNICATIONS, INSTITUTION OF ELECTRICAL ENGINEERS, GB, vol. 147, no. 6, 11 December 2000 (2000-12-11), pages 345-350, XP006014002 ISSN: 1350-2425 page 345 ---	1-19
A	RIVEST R L ET AL: "PAY WORD AND MICROMINT: TWO SIMPLE MICROPAYMENT SCHEMES" SECURITY PROTOCOLS. INTERNATIONAL WORKSHOP PROCEEDINGS, XX, XX, 1997, pages 69-87, XP000677143 page 70 -page 74 -----	1-19

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 03/03380

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	KOBAYASHI K; MORITA H: "EFFICIENT SEALED-BID AUCTION BY USING ONE-WAY FUNCTIONS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, INSTITUTE OF ELECTRONICS INFORMATION AND COMM. ENG. , vol. e84-A, no. 1, 1 janvier 2001 (2001-01-01), pages 289-294, XP001006551 TOKYO, JP page 289 page 291, colonne de gauche -page 293, colonne de gauche --- -/--	1-19

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
27 avril 2004	07/05/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 03/03380

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	SUZUKI K ; KOBAYASHI K ; MORITA H : "Efficient sealed-bid auction using hash chain" INFORMATION SECURITY AND CRYPTOLOGY - ICISC 2000. THIRD INTERNATIONAL CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2015, SPRINGER VERLAG), 9 décembre 2000 (2000-12-09), pages 183-191, XP002247412 Seoul, South Korea ISBN: 3-540-41782-6 page 183 page 185 -page 189	1-19
X	BYOUNGCHEON LEE; KWANGJO KIM; JOONGSOO MA: "Efficient Public Auction with One-Time Registration and Public Verifiability" INDOCRYPT 2001, SECOND INTERNATIONAL CONFERENCE ON CRYPTOLOGY IN INDIA, 'en ligne! 16 - 20 décembre 2001, pages 162-174, XP002247413 Indian Institute of Technology, Madras, Chennai, India Extrait de l'Internet: <URL:http://citeseer.nj.nec.com/cs> 'extrait le 2003-07-04! page 166 -page 172	1-19
A	ZHANG N ET AL: "Anonymous public-key certificates for anonymous and fair document exchange" IEE PROCEEDINGS: COMMUNICATIONS, INSTITUTION OF ELECTRICAL ENGINEERS, GB, vol. 147, no. 6, 11 décembre 2000 (2000-12-11), pages 345-350, XP006014002 ISSN: 1350-2425 page 345	1-19
A	RIVEST R L ET AL: "PAY WORD AND MICROMINT: TWO SIMPLE MICROPAYMENT SCHEMES" SECURITY PROTOCOLS. INTERNATIONAL WORKSHOP PROCEEDINGS, XX, XX, 1997, pages 69-87, XP000677143 page 70 -page 74	1-19